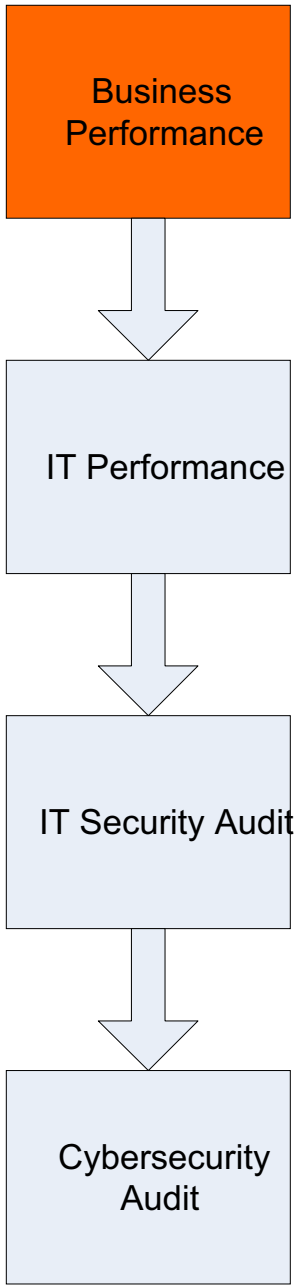
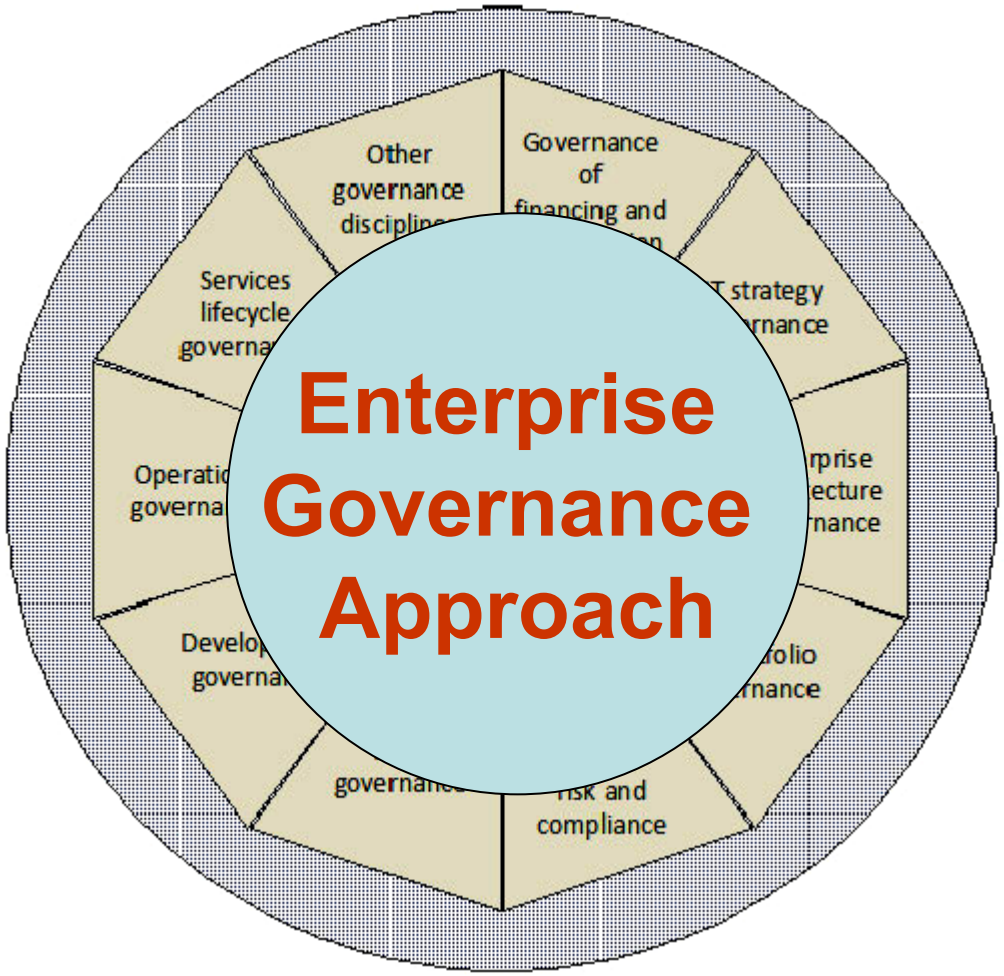
Cybersecurity Audit

Part 1 – IT Audit

TTÜ 2008

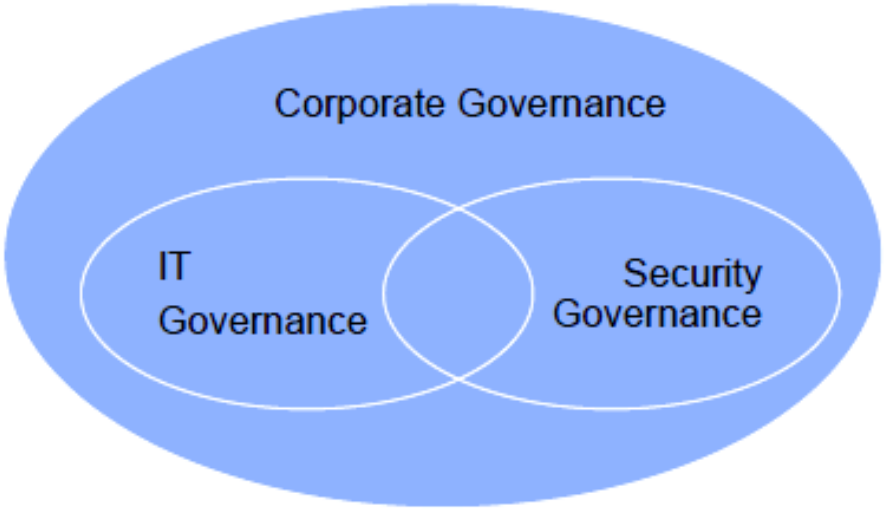

Business Performance
IT Performance
IT Security Audit
Cybersecurity Audit

Sample IT Governance Landscape



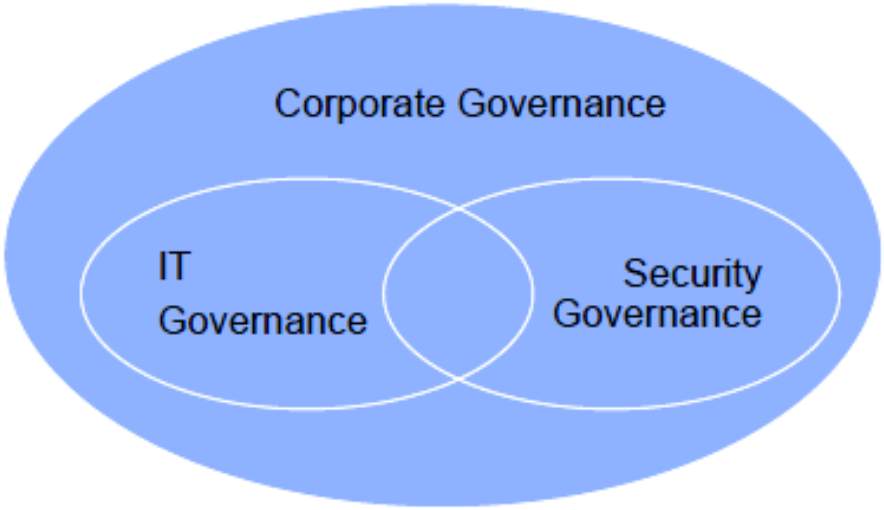
Sample IT Governance Landscape

Enterprise, IT and Information Security Governance Relationships



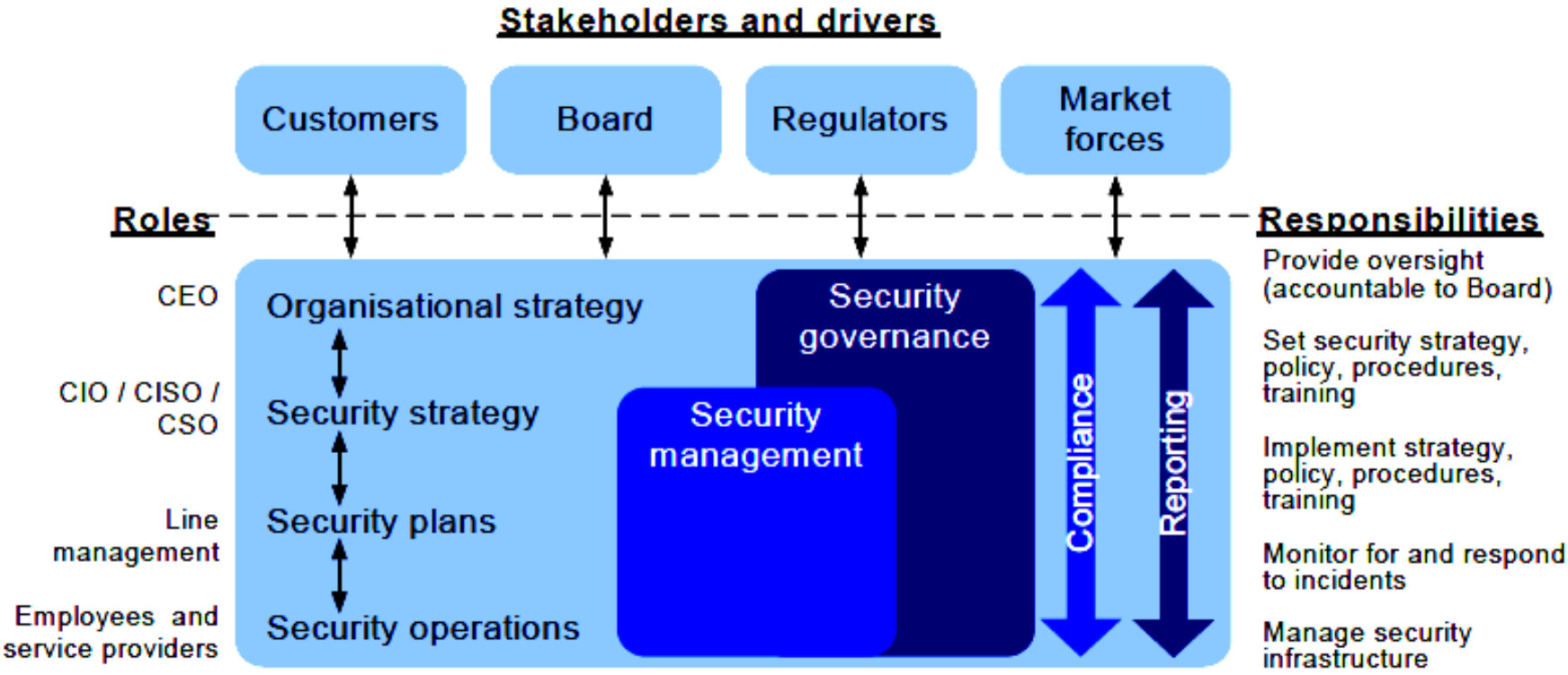
IT governance provides outcomes specifically focused on aligning IT with the business while security governance provides outcomes specifically focused on aligning security with the business.

Enterprise, IT and Information Security Governance Relationships

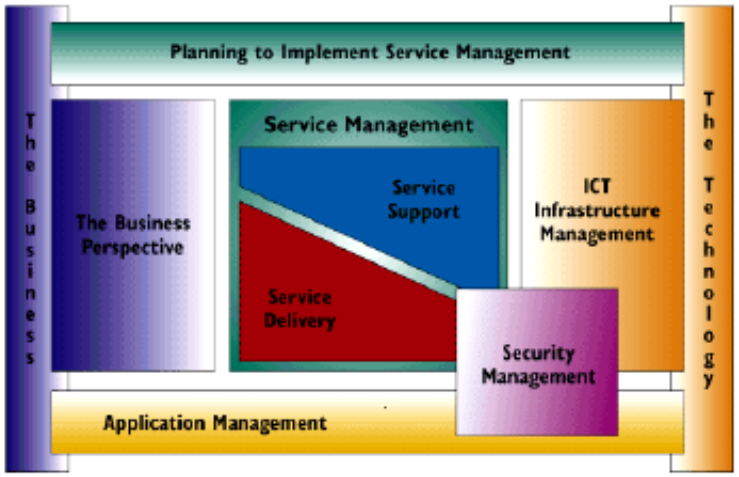


Security governance provides outcomes specifically focused on aligning security with the business.

Information Security Governance Framework

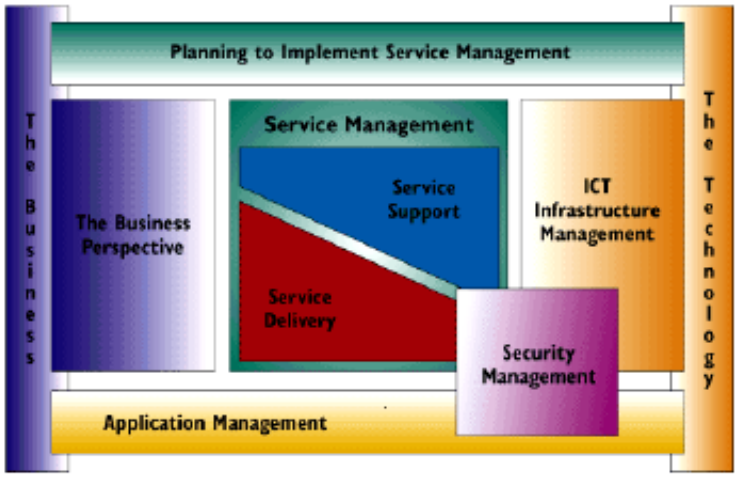


From ITILv2 to ITILv3



ITIL v2 Publication Framework

From ITILv2 to ITILv3



ITIL v2 Publication Framework

ITIL v3 Service Lifecycle

itSMF International

The IT Service Management Forum

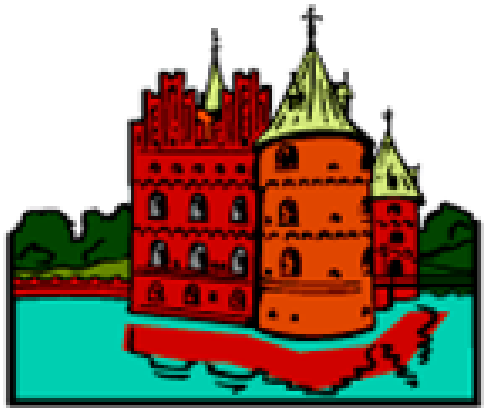
- **Service Strategy**
- **Service Design**
- **Service Transition**
- **Service Operation**
- **Continual Service Improvement**

The Fortress Mentality

Country in which there are precipitous cliffs with torrents running between, deep natural hollows, confined places, tangled thickets, quagmires and crevasses, should be left with all possible speed and not approached.

The Fortress Mentality

- In past centuries, armies built fortresses as a major part of their military strategy.
- Fortresses had different architectures, defense features, and so forth, and for a while they worked.
- Then came the advent of more powerful weaponry.
- Troops that stayed inside fortresses eventually became sitting ducks.
- Fortresses are now not much more than items of curiosity in the twenty-first century.




ISM3

Traditional Approach to Security:

- "**We want to prevent attacks from succeeding**". With this approach, to be secure means to be *invulnerable*.

Traditional Approach to Security:

- "**We want to prevent attacks from succeeding**". With this approach, to be secure means to be *invulnerable*.
- An incident is any loss of confidentiality, integrity or availability.

Traditional Approach to Security:

- "**We want to prevent attacks from succeeding**". With this approach, to be secure means to be *invulnerable*.
- An incident is any loss of confidentiality, integrity or availability.
- You look at a piece of data and think: Is it confidential, has it got integrity, is it available?

ISM3 Approach

- "**We want to guarantee that our business goals are met**". With this approach, to be secure means to be reliable, despite attacks, accidents and errors.

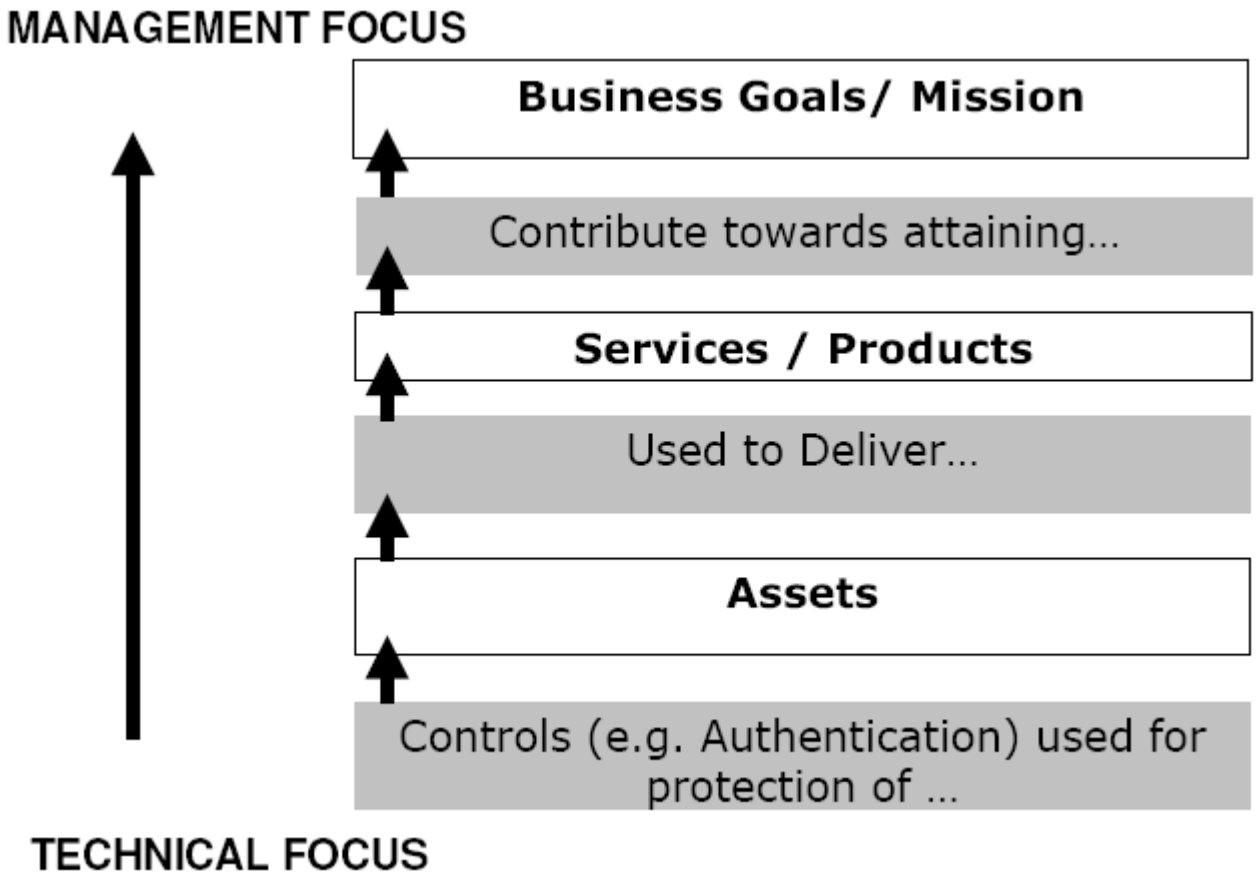
ISM3 Approach

- "**We want to guarantee that our business goals are met**". With this approach, to be secure means to be reliable, despite attacks, accidents and errors.
- An incident is a failure to meet a security objective resulting from accidents, errors or attacks.

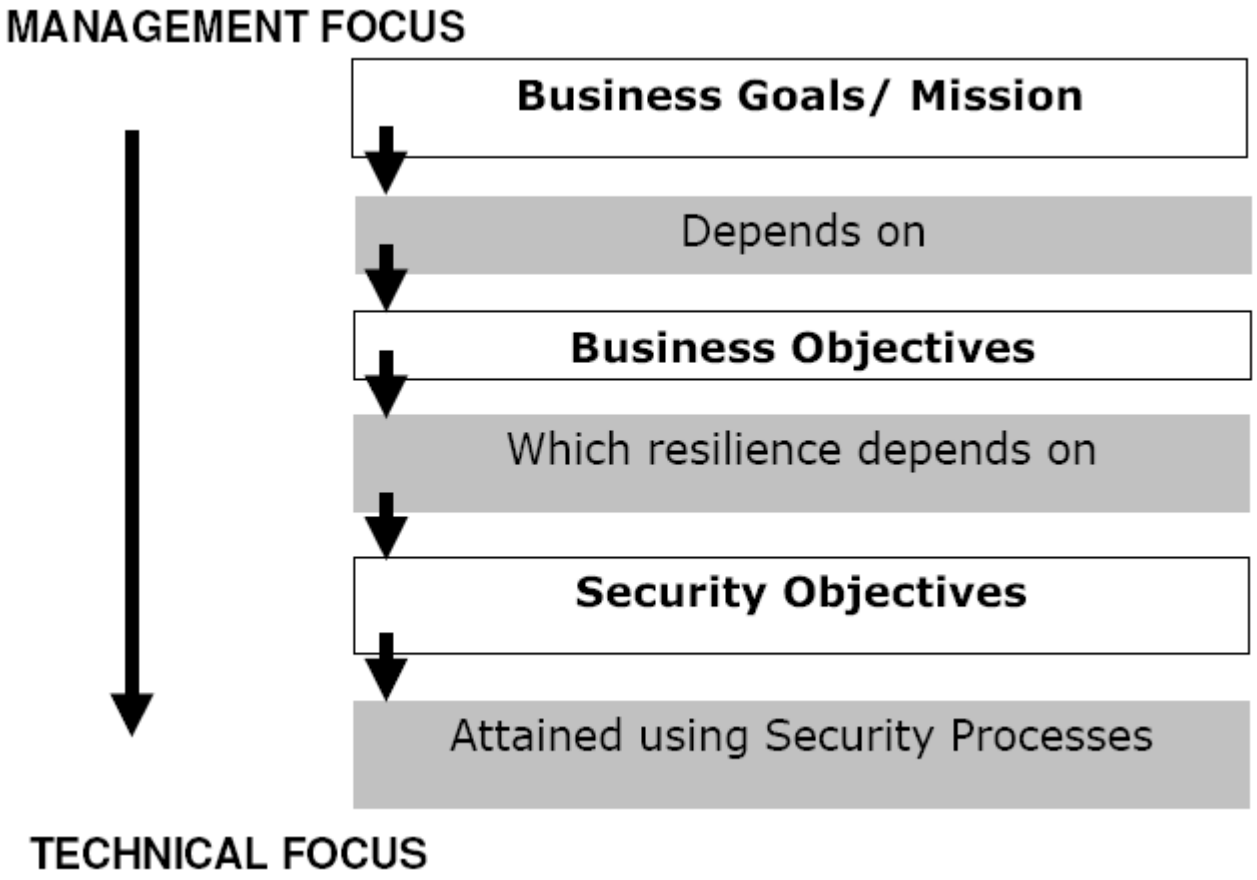
ISM3 Approach

- "**We want to guarantee that our business goals are met**". With this approach, to be secure means to be reliable, despite attacks, accidents and errors.
- An incident is a failure to meet a security objective resulting from accidents, errors or attacks.
- Using ISM3 you look at a piece of data and think: What properties of this data must be protected for it to have business value?

Traditional Approach



ISM3 Business Focus




Our Disaster Recovery Plan Goes Something Like This...
HELP! HELP!
DILBERT
By Scott Adams

Business Continuity Management: Standards and Guidelines

- PAS77/BS 25777 (ITSC - UK)
- NIST 800-34 (ITSC - USA)
- ISO 27001 (IS -International)
- BSI 100-2 (IS - Germany)
- COBiT 4 (IT - USA)
- ITIL 2 & 3 (IT – UK)
- BS ISO IEC 24762 (DR – International
- BS 25999 (BCM - UK)
- BCI GPG (BCM – UK)
- HB 221 (BCM – Aus & NZ)
- HB 292 (BCM – Aus & NZ)
- HB 293 (BCM – Aus & NZ)
- APS 232 (BCM – Aus & NZ)
- TR 19 (BCM –Singapore)
- NFPA 1600 (EM – USA)
- FEMA 141 (EM – USA)
- ISO PAS 22399 (EM/BCM – International)
- Basel II
- Sarbanes Oxley

Business Continuity Management: Standards and Guidelines

- **PAS77/BS 25777 (ITSC - UK)**
- **NIST 800-34 (ITSC - USA)**
- **ISO 27001 (IS -International)**
- BSI 100-2 (IS - Germany)
- **COBiT 4 (IT - USA)**
- **ITIL 2 & 3 (IT – UK)**
- BS ISO IEC 24762 (DR – International
- **BS 25999 (BCM - UK)**
- BCI GPG (BCM – UK)
- HB 221 (BCM – Aus & NZ)
- HB 292 (BCM – Aus & NZ)
- HB 293 (BCM – Aus & NZ)
- APS 232 (BCM – Aus & NZ)
- TR 19 (BCM –Singapore)
- NFPA 1600 (EM – USA)
- FEMA 141 (EM – USA)
- ISO PAS 22399 (EM/BCM – International)
- **Basel II**
- **Sarbanes Oxley**

Version 6.1

British Standar

Head Office
389 Chiswick High Roa
London W4 4AL
Telephone: +44(0)20 899
Fax: +44(0)20 8996 7001
www.bsi-global.com

British Standards

Head Office
389 Chiswick High Road
London W4 4AL
Telephone: +44(0)20 8996 9000
Fax: +44(0)20 8996 7001
www.bsi-global.com

Version 6.1 '30139869 DC

DPC: 06/30139869 DC

Date: 23 June 2006 2006
Origin: National tional

Latest date for receipt of comments: 31 August 2006 Project no.: 2005/02478
Responsible committee: BCM/1

Interested committees:

Latest date for rec .: 2005/02478
Responsible comm

BS 25999-1 Code of practice for business continuity management

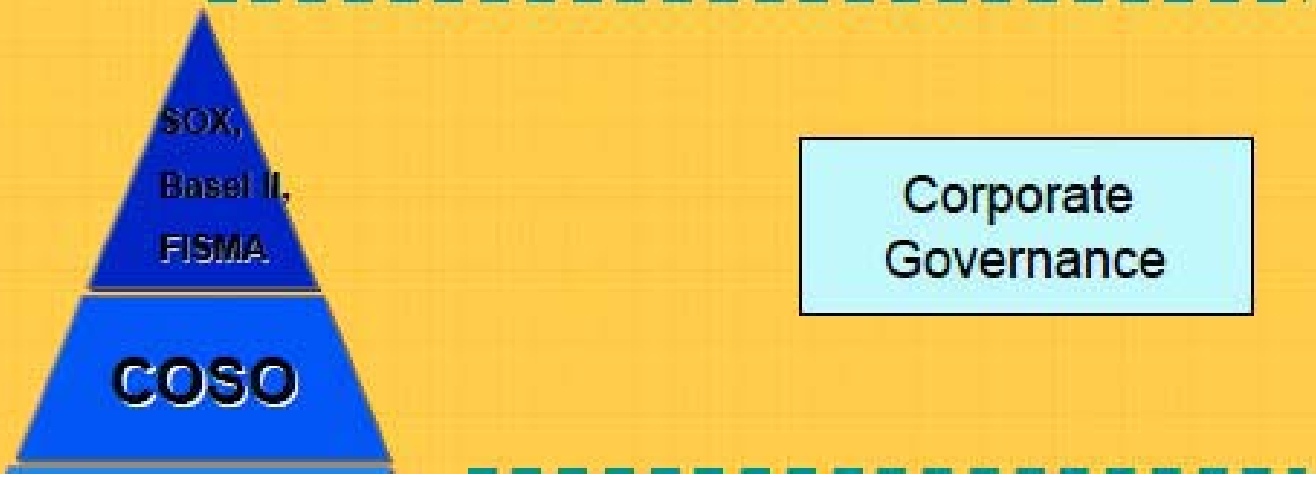
Title: DPC BS

Supersession information: If this document is published as a standard, the UK implementation of it will supersede NONE and partially supersede NONE . If you are aware of a current national standard which may be affected, please notify the content developer (contact details below).

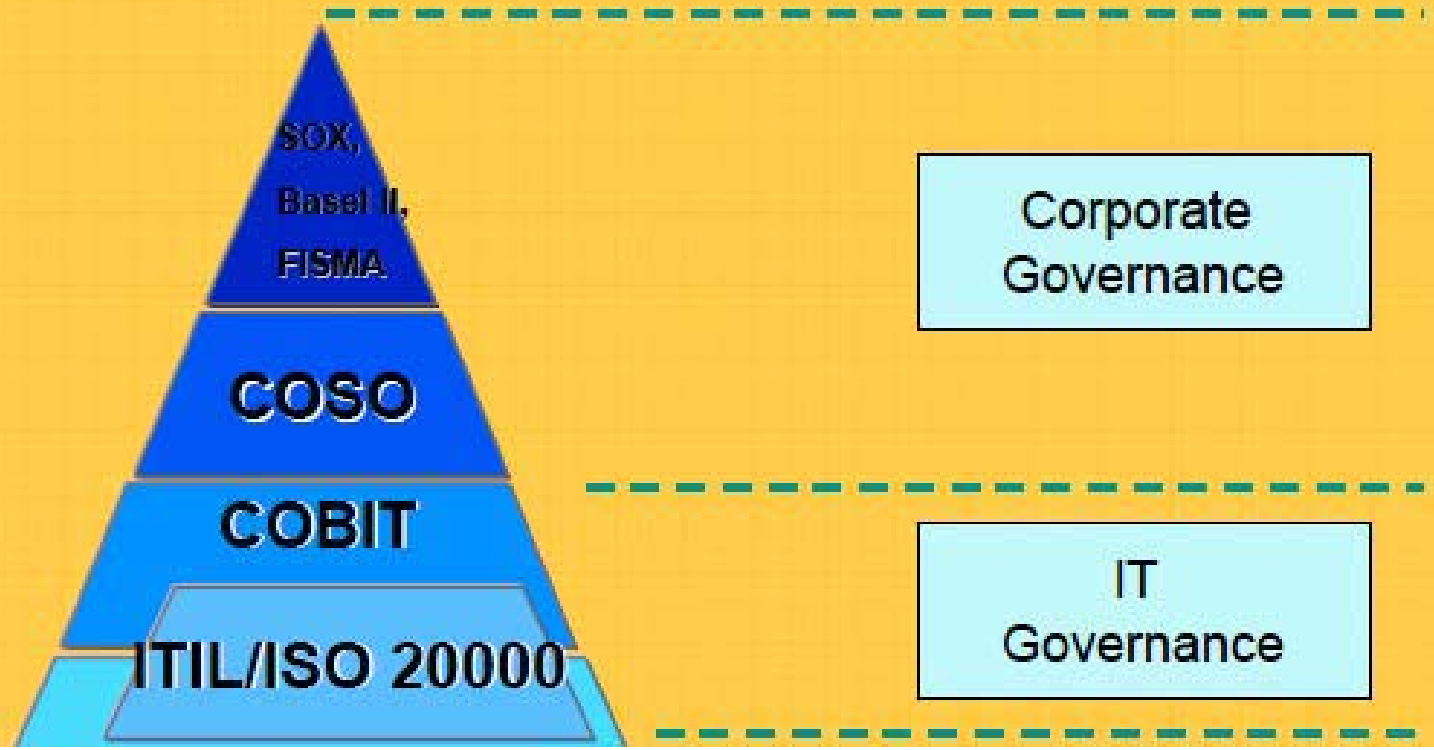
Governance and "Standards"

Corporate Governance

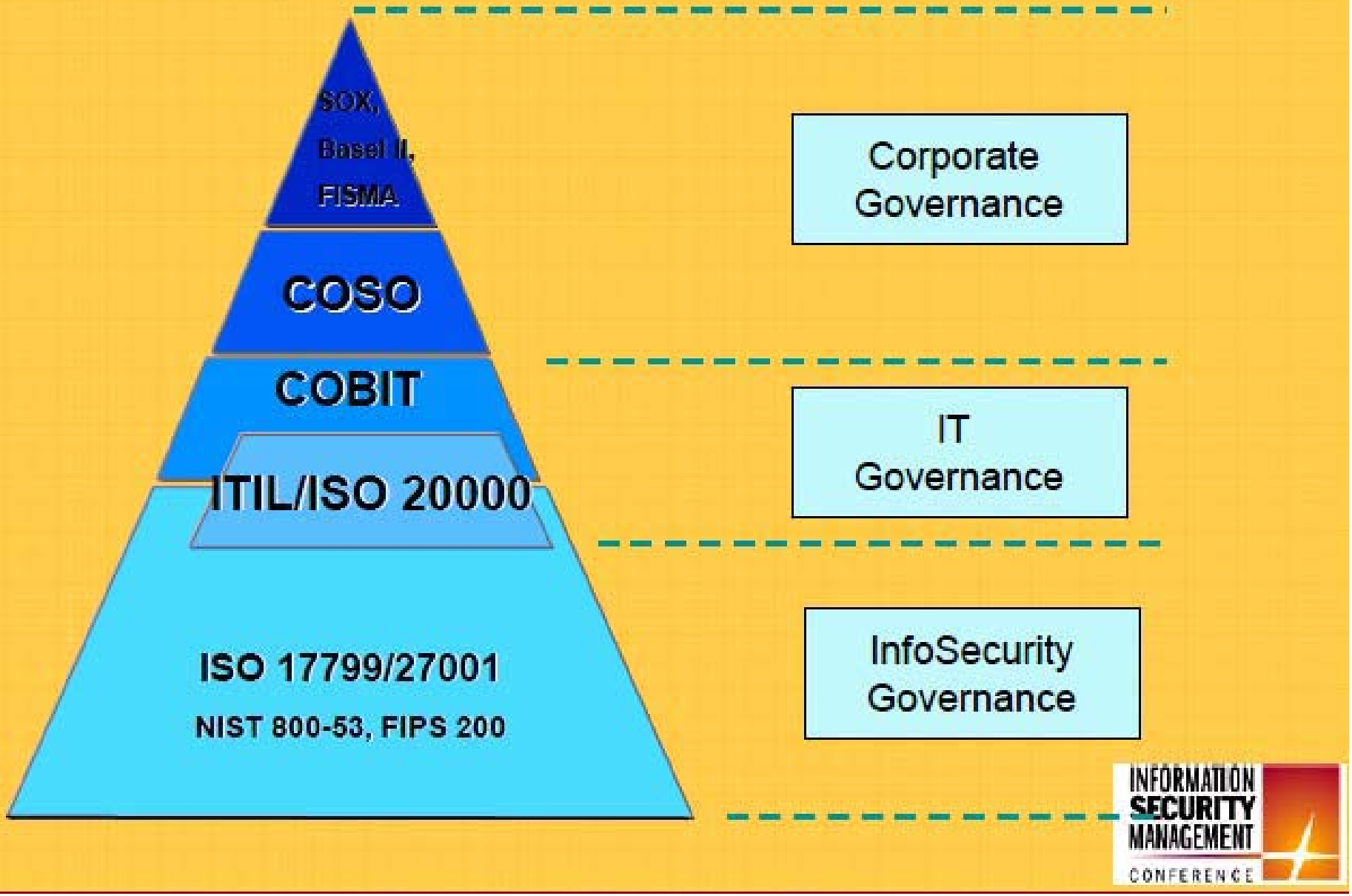
Governance and "Standards"



Governance and "Standards"

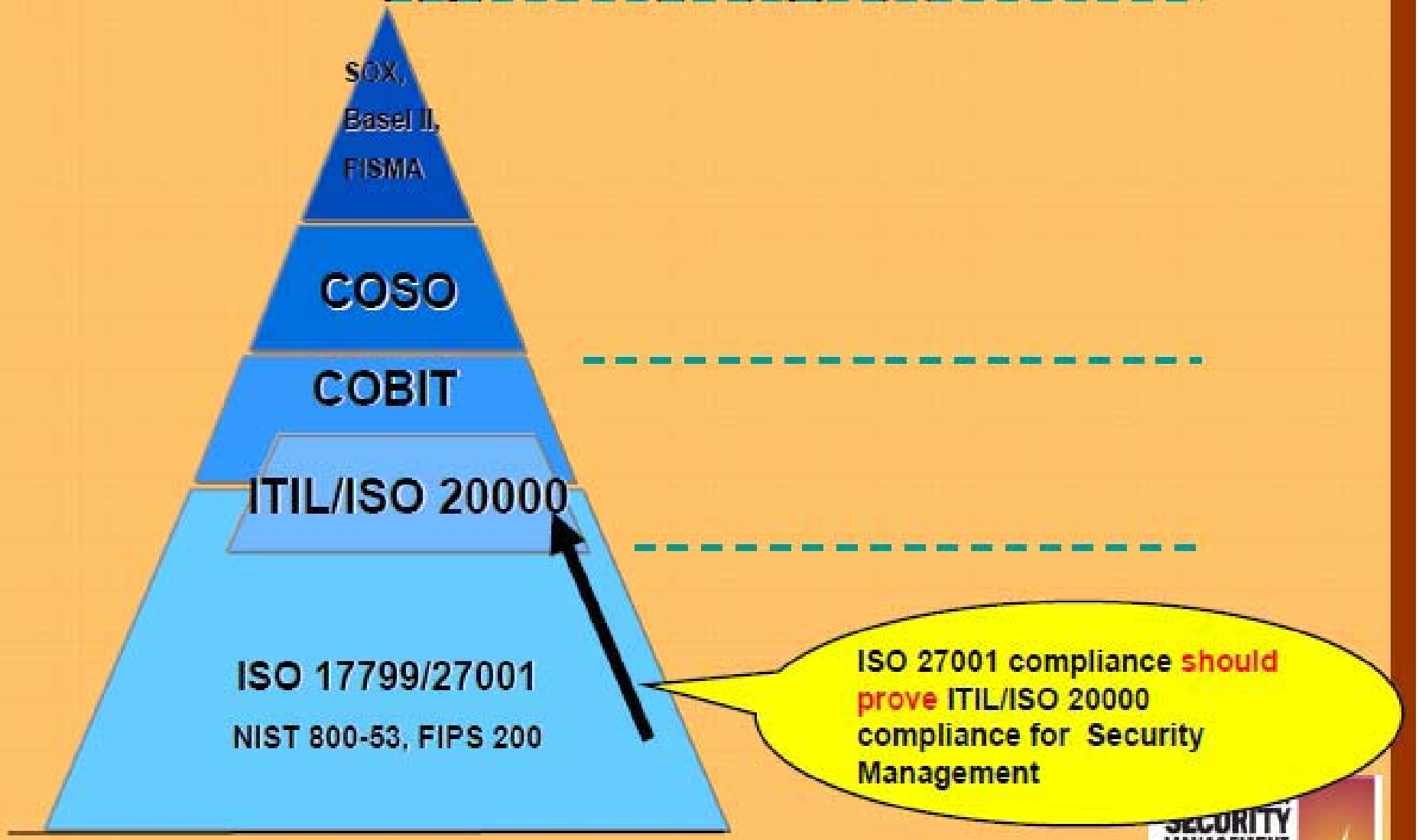


Governance and "Standards"

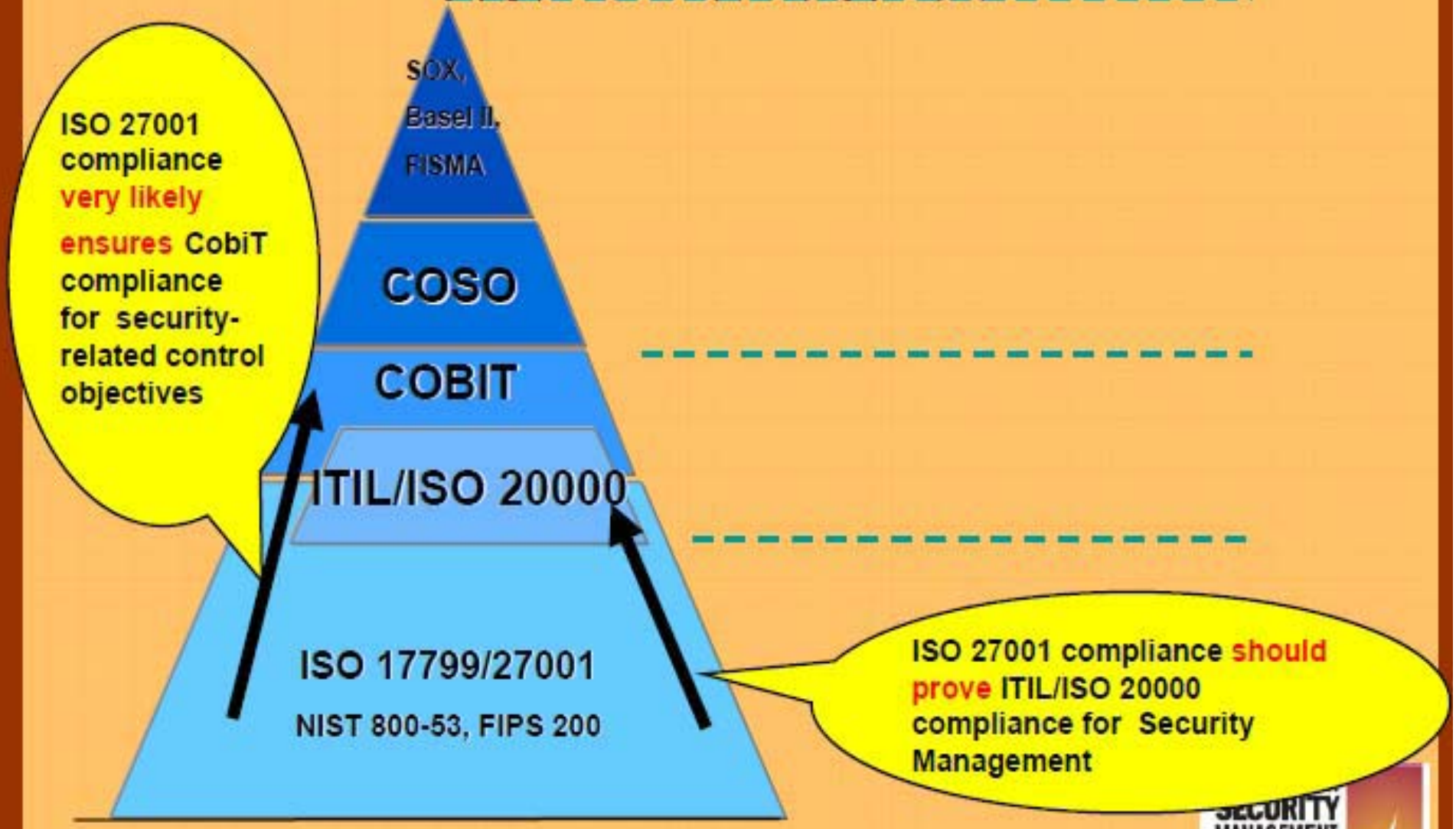


INFORMATION SECURITY MANAGEMENT CONFERENCE

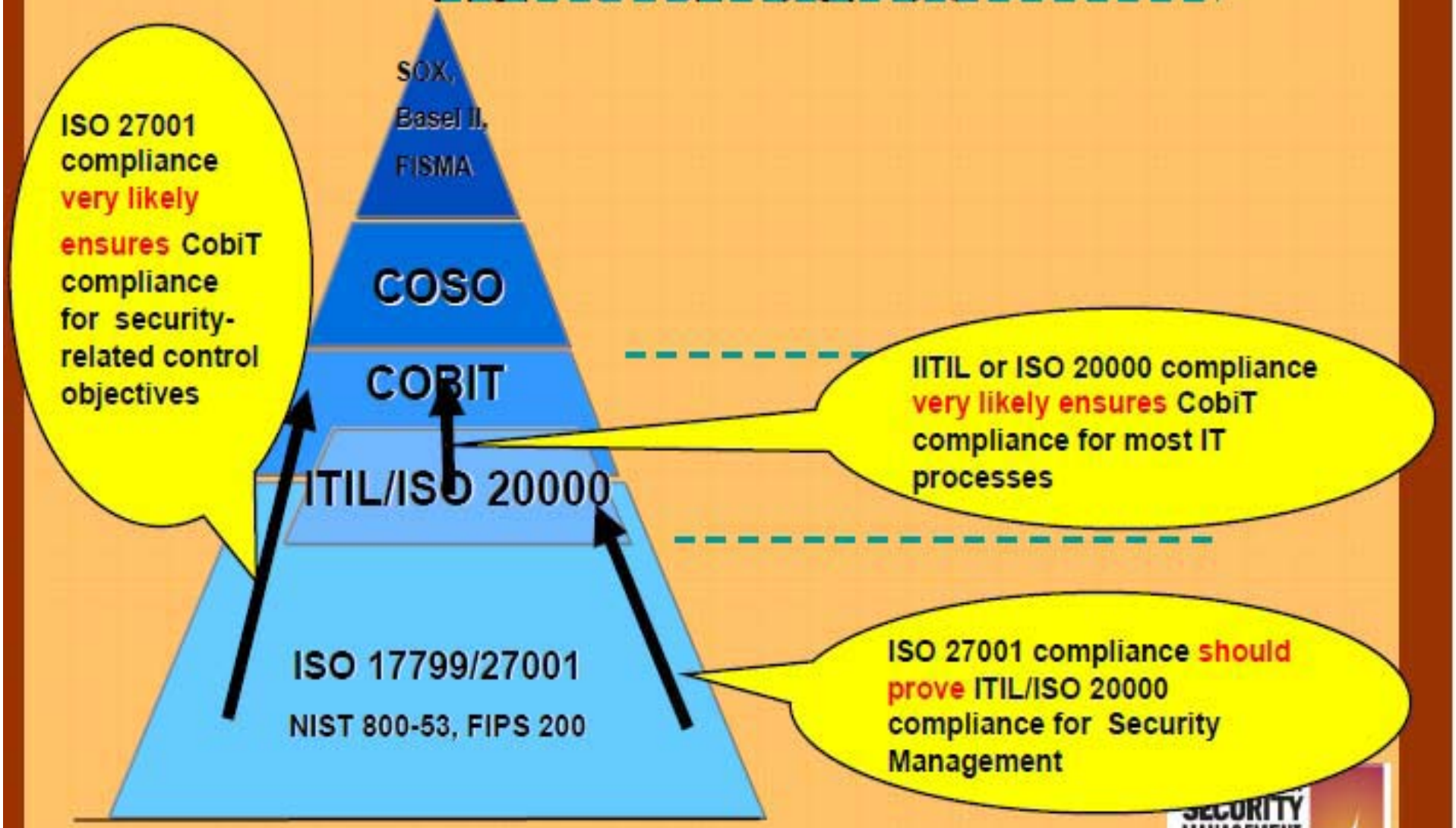
Achieving upward compliance via "standards"



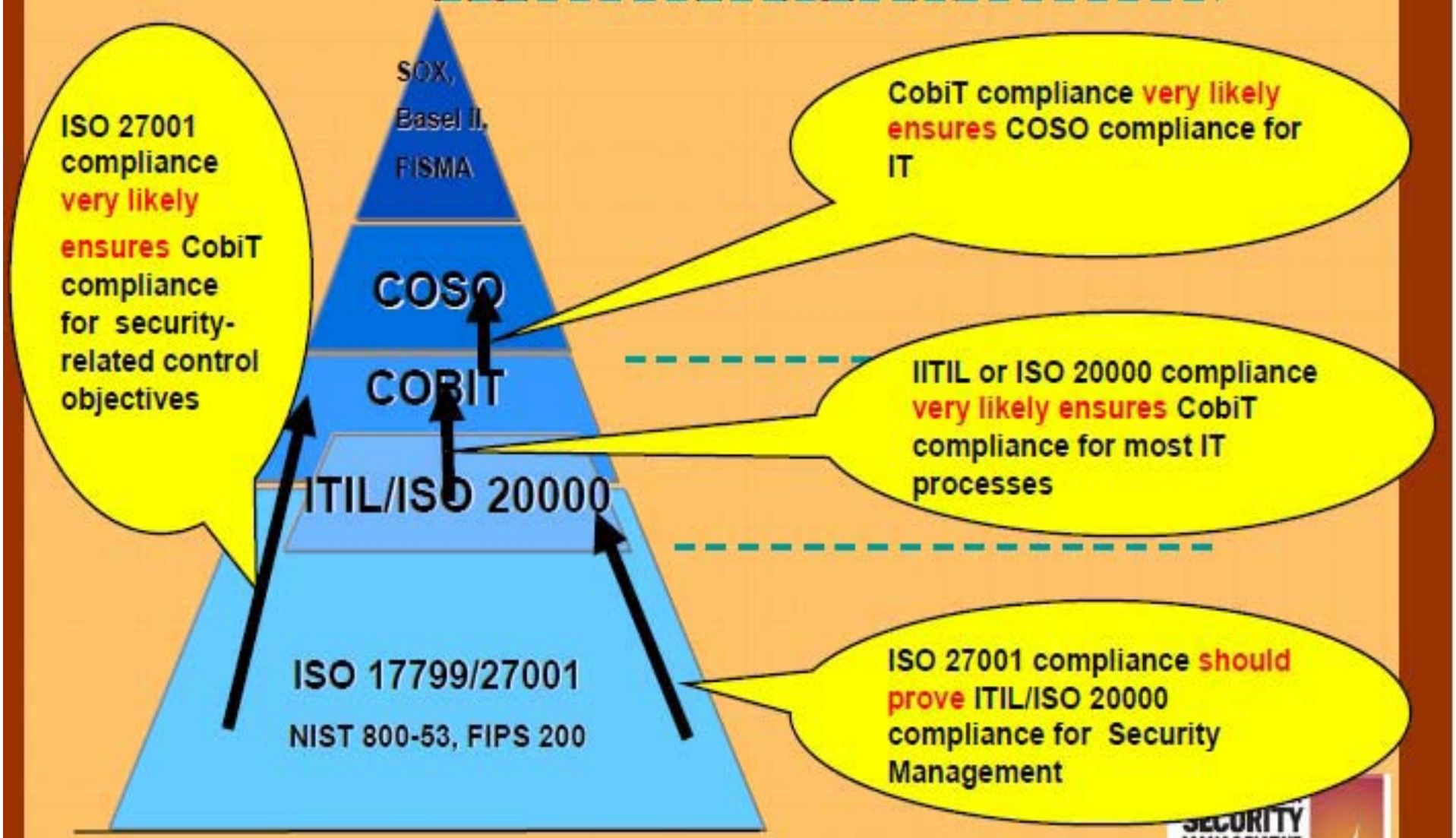
Achieving upward compliance via "standards"



Achieving upward compliance via "standards"

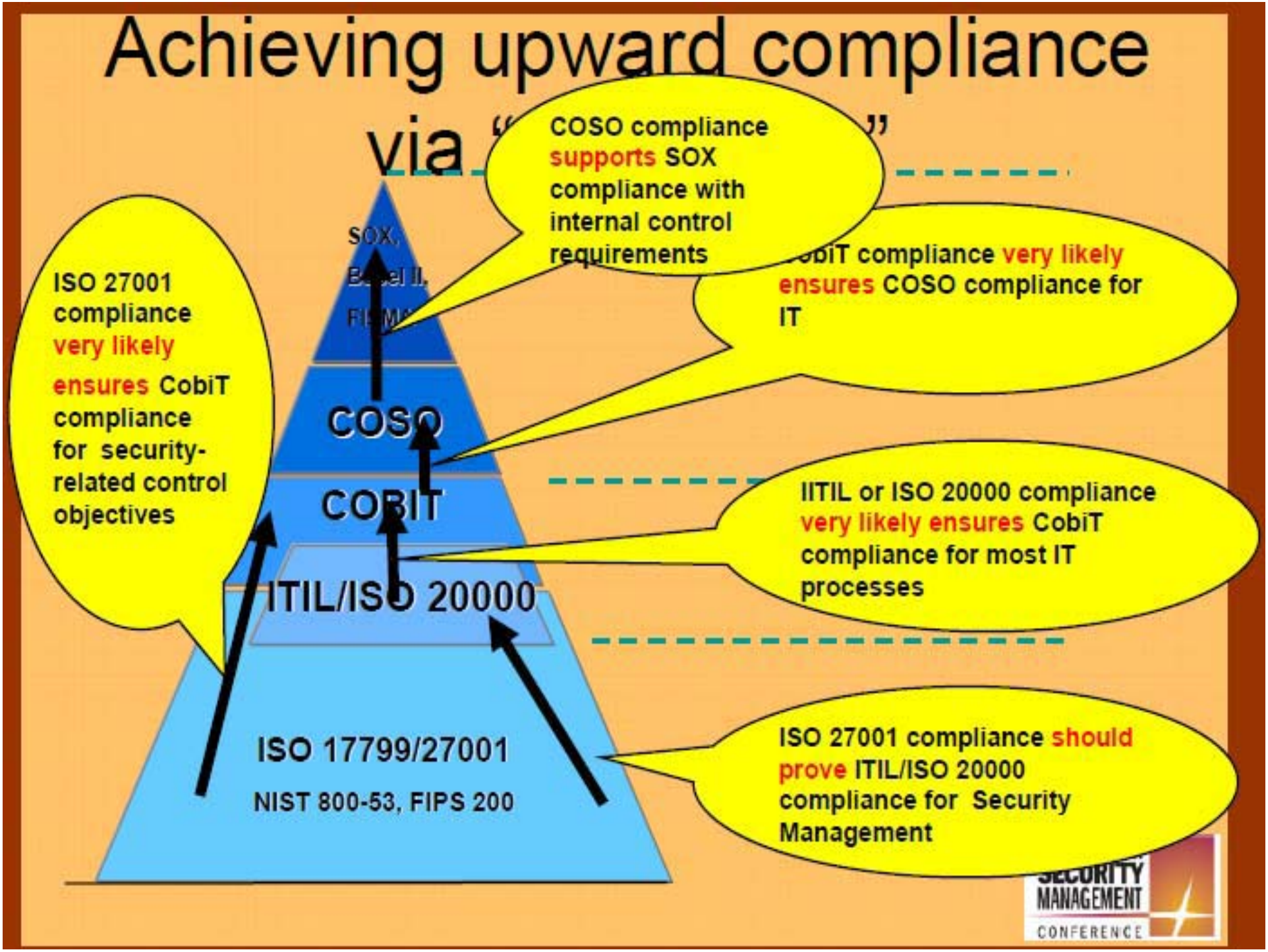


Achieving upward compliance via "standards"

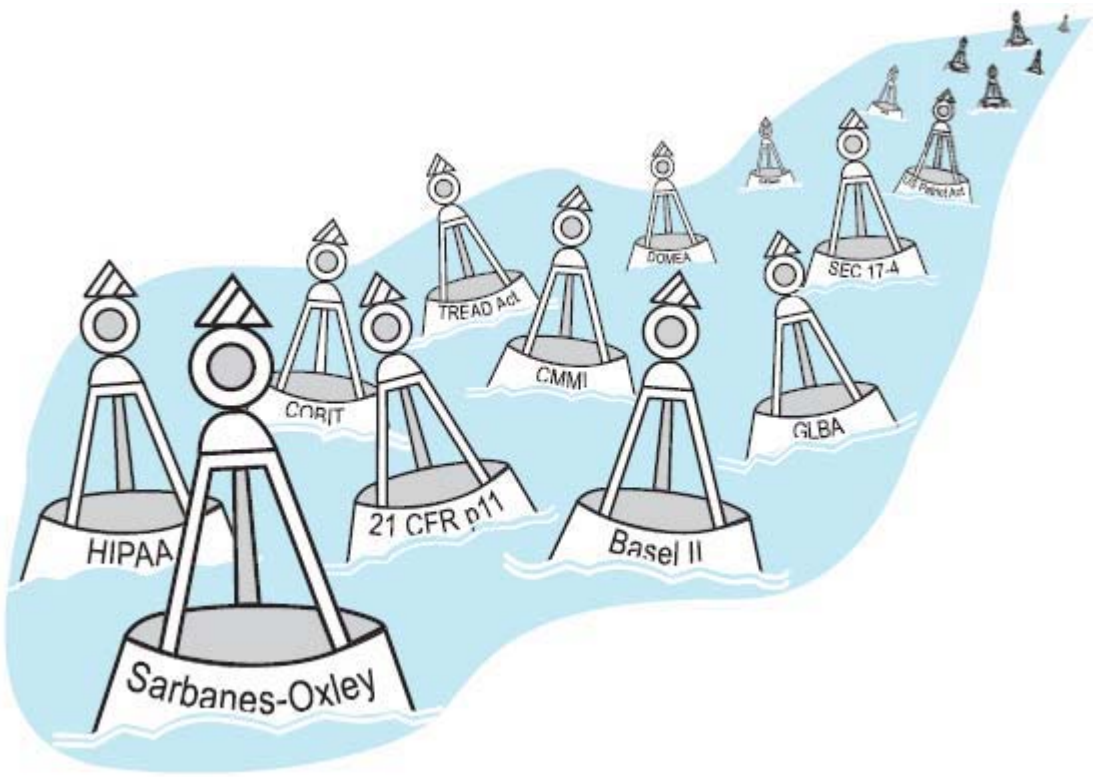


SECURITY MANAGEMENT CONFERENCE

Achieving upward compliance via "

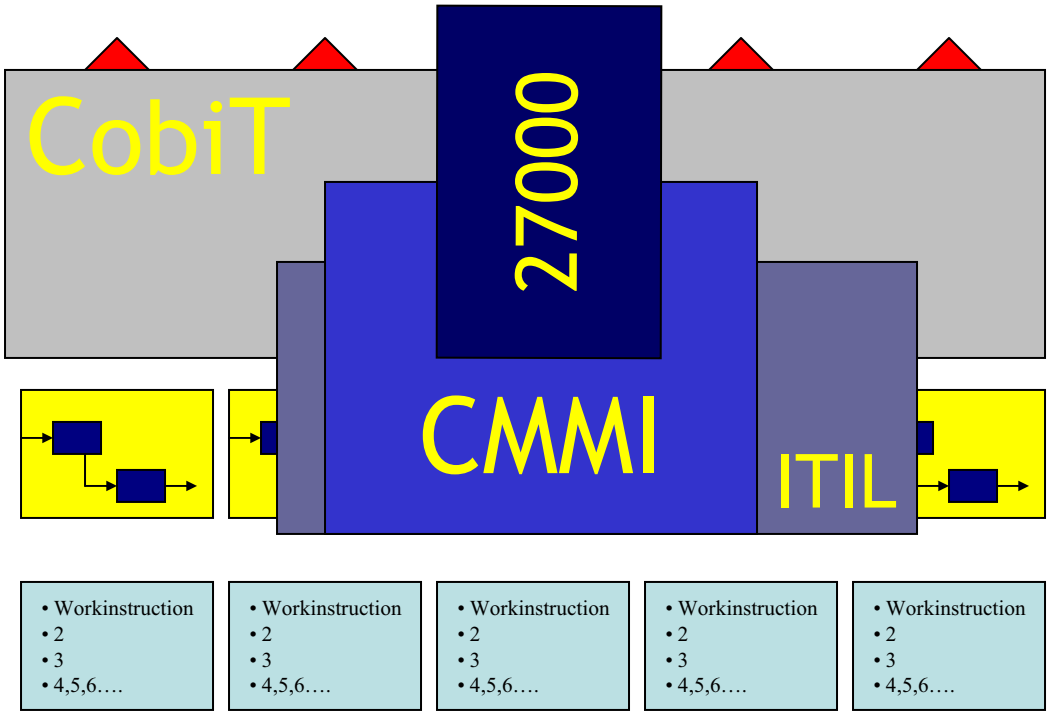


Sea of Regulations and Standards

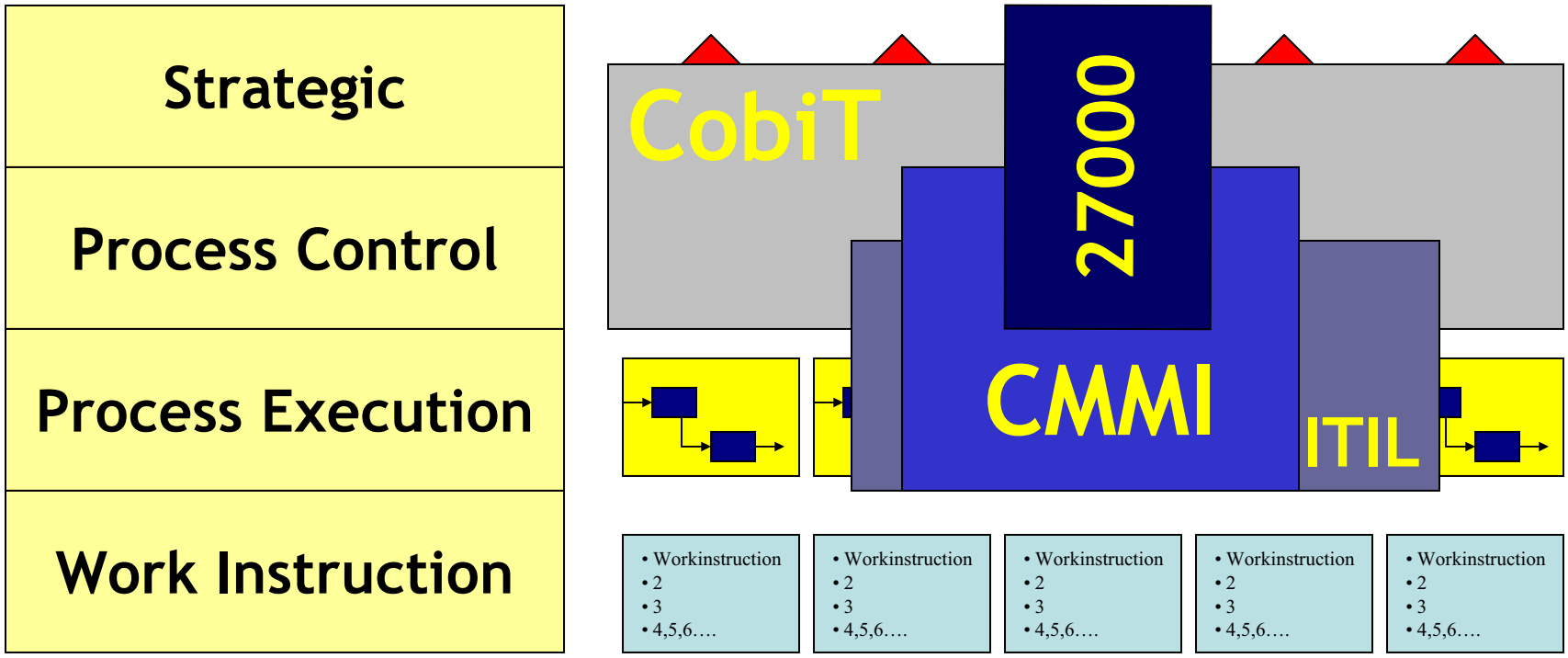


How CobiT Relates to Frameworks and Standards

Strategic
Process Control
Process Execution
Work Instruction



How CobiT Relates to Frameworks and Standards



Miks auditist?

Audit on IT juhtimises oluliseks instrumendiks:

- Mittevastavuste õigeaegne avastamine võimaldab korrigeerivate ja preventiivsete toimingute abil leevendada IT riske
- IT toimimise parendamine
- …

The Audit Function

- The audit is to examine and to assure.
- The nature of auditing differs according to the subject under examination.
- Audits can be
  - internal,
  - external, and
  - audits of information systems.

Internal versus External Auditing

- In an internal audit a company's own accounting employees perform the audit.
- Accountants working for an independent firm normally perform the external audit.

External Audits

- External auditing: Objective is that in all material respects, financial statements are a fair representation of organization's transactions and account balances.
  - Sarbanes-Oxley Act
  - etc

Internal Audits

- Internal auditing: independent appraisal function established within an organization to examine and evaluate its activities as a service to the organization
- Financial Audits
- Operational Audits
- Compliance Audits
- Fraud Audits
- IT Audits

IT Security

IT Security is

... Not an event

…Not a milestone

… Not a Technology

IT Security

IT Security is

... Not an event

…Not a milestone

… Not a Technology

IT Security is a process

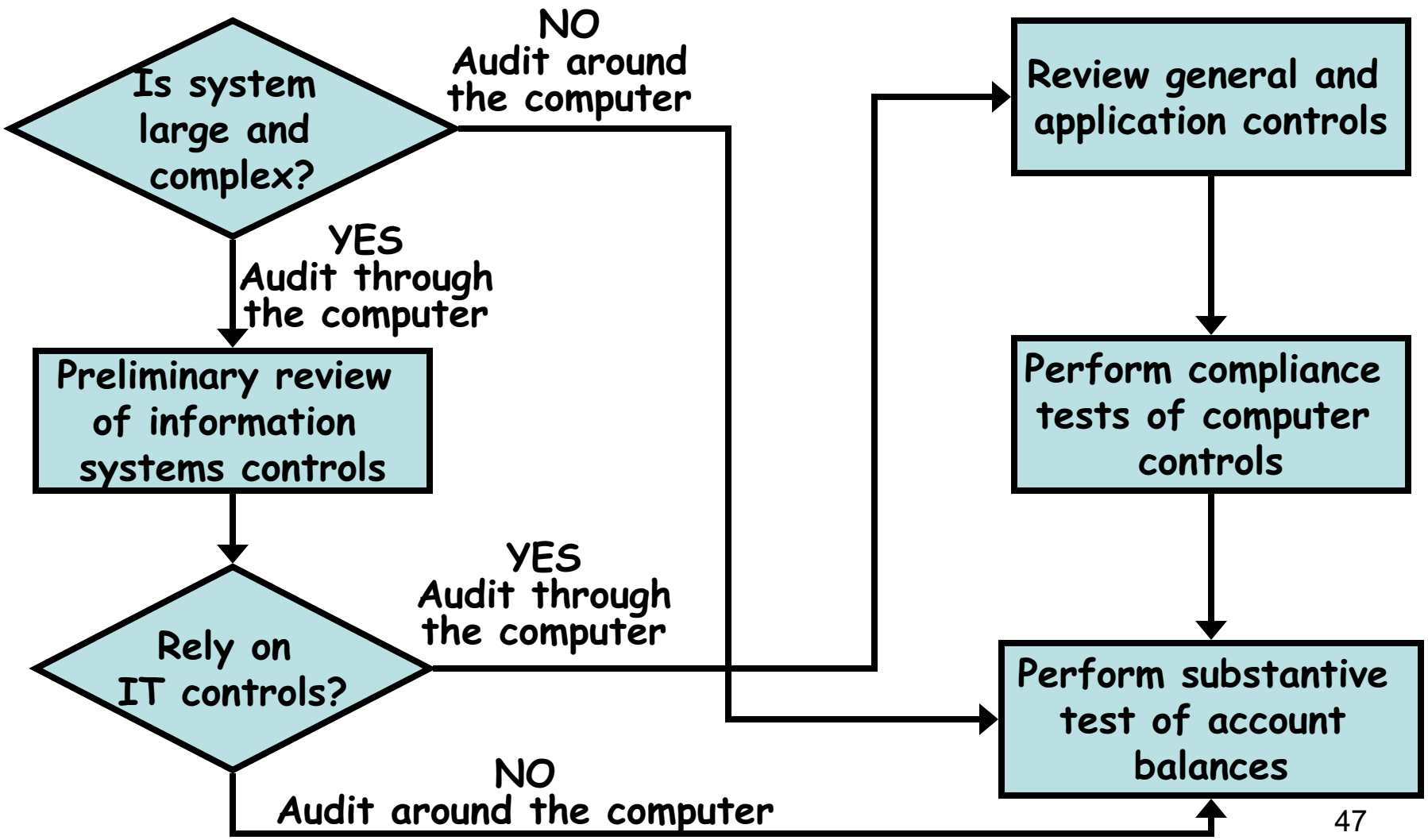
IT Audits

- IT audits: provide audit services where processes or data, or both, are embedded in technologies.
  - Subject to ethics, guidelines, and standards of the profession (if certified)
    - CISA
    - Most closely associated with ISACA
  - Joint with internal, external, and fraud audits
  - Scope of IT audit coverage is increasing
  - IT governance as part of corporate governance

Information Systems Auditing

- Information systems auditing or *electronic data processing* (EDP) auditing involves evaluating the computer's role in achieving audit and control objectives.
- The AIS components of a computer-based AIS are people, procedures, hardware, data communications, software and databases.
- These components are a system of interacting elements.

Information Systems Audit Process

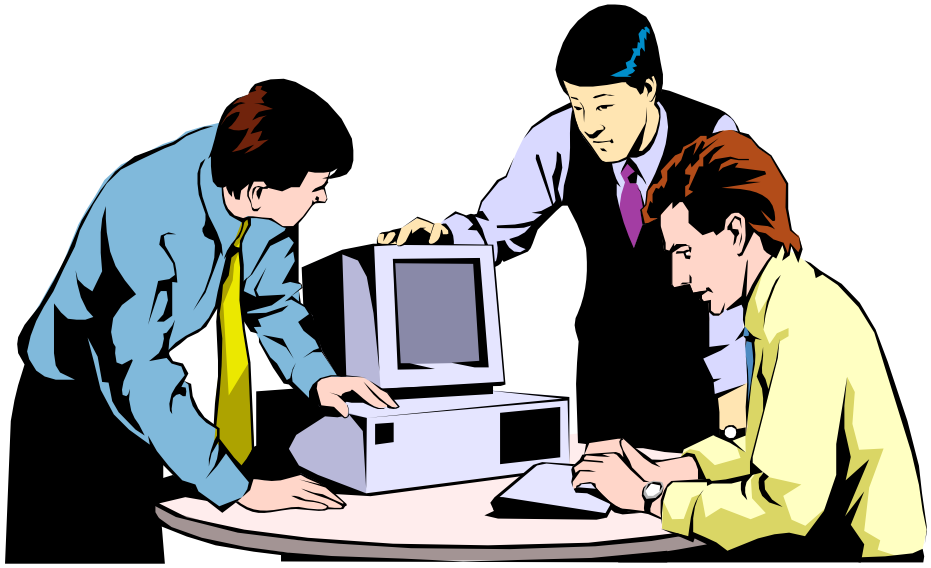


Fraud Audits

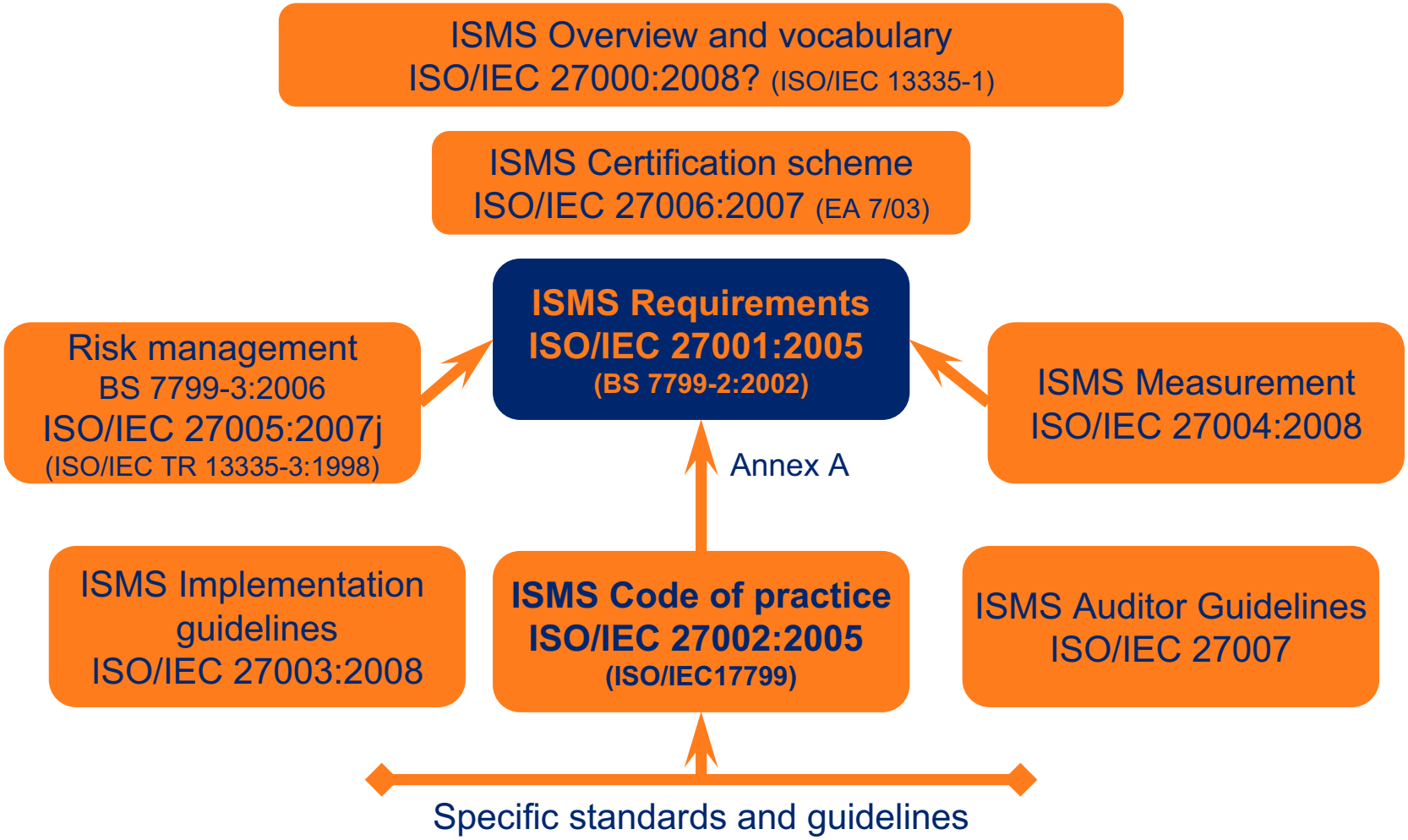
- Fraud audits: provide investigation services where anomalies are suspected, to develop evidence to support or deny fraudulent activities.
  - Auditor is more like a detective
  - No materiality
  - Goal is conviction, if sufficient evidence of fraud exists

Evaluating the Effectiveness of IT Controls Risk Assessment

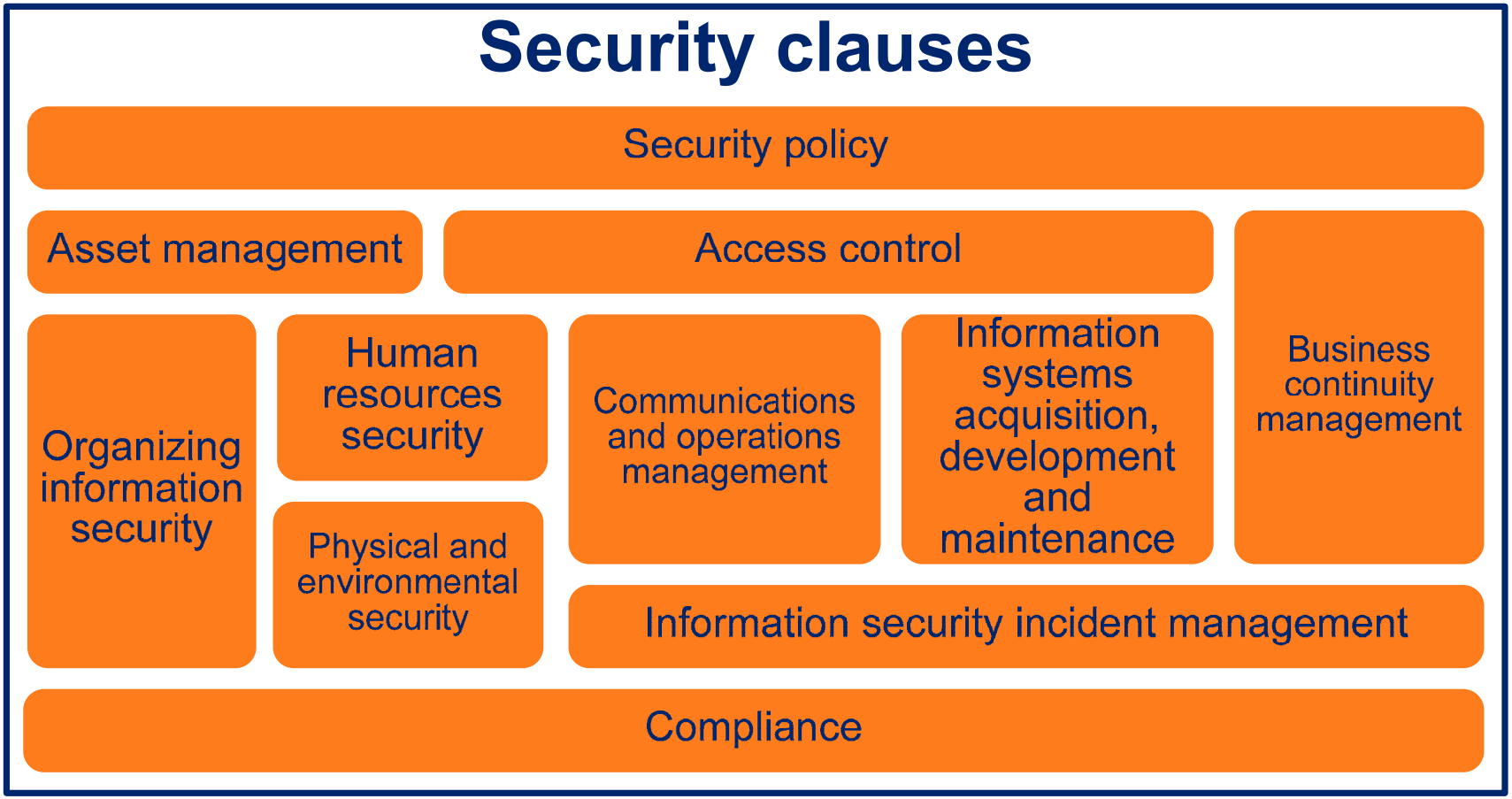
- External auditor's main objective in reviewing information systems control procedures is to evaluate the risks to the integrity of accounting data.
- Information Systems Risk Assessment is a method for evaluating the desirability of IT-related controls for a particular aspect of business risk.



ISO/IEC 27000 Family Review



Structure of ISO/IEC 27002:2005 (ISO/IEC 17799)



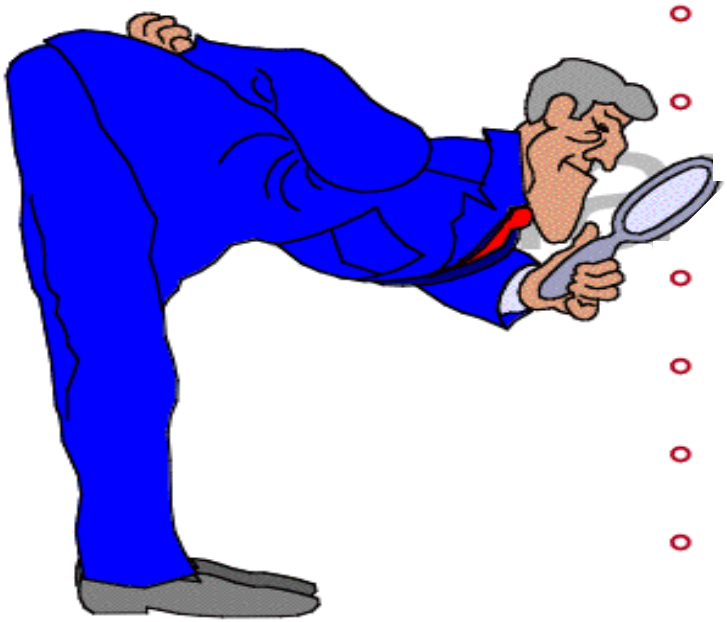
Auditeerimisprotsess

Eriti lühike auditikoodeks

- Auditeerimine pole mõnus –
  eriti auditeeritavale
- Mõlemad osapooled, nii *auditeerija* kui ka *auditeeritav* peavad teadma mitte ainult seda,
  mida teha, vaid ka seda,
  mida **mitte** teha

“Hirm auditi ees”

- **Auditeeritav**:
  Ära lase ennast tabada “püksid rebadel”
- Auditeeritaval on auditist kasu –
  KUI AUDIT ON TEHTUD KORREKTSELT



Auditeerimise tehnikad

- Plaanimine
- Kontroll-listid
- Auditi tähelepanekud
- Auditi raportid

Auditi eesmärk

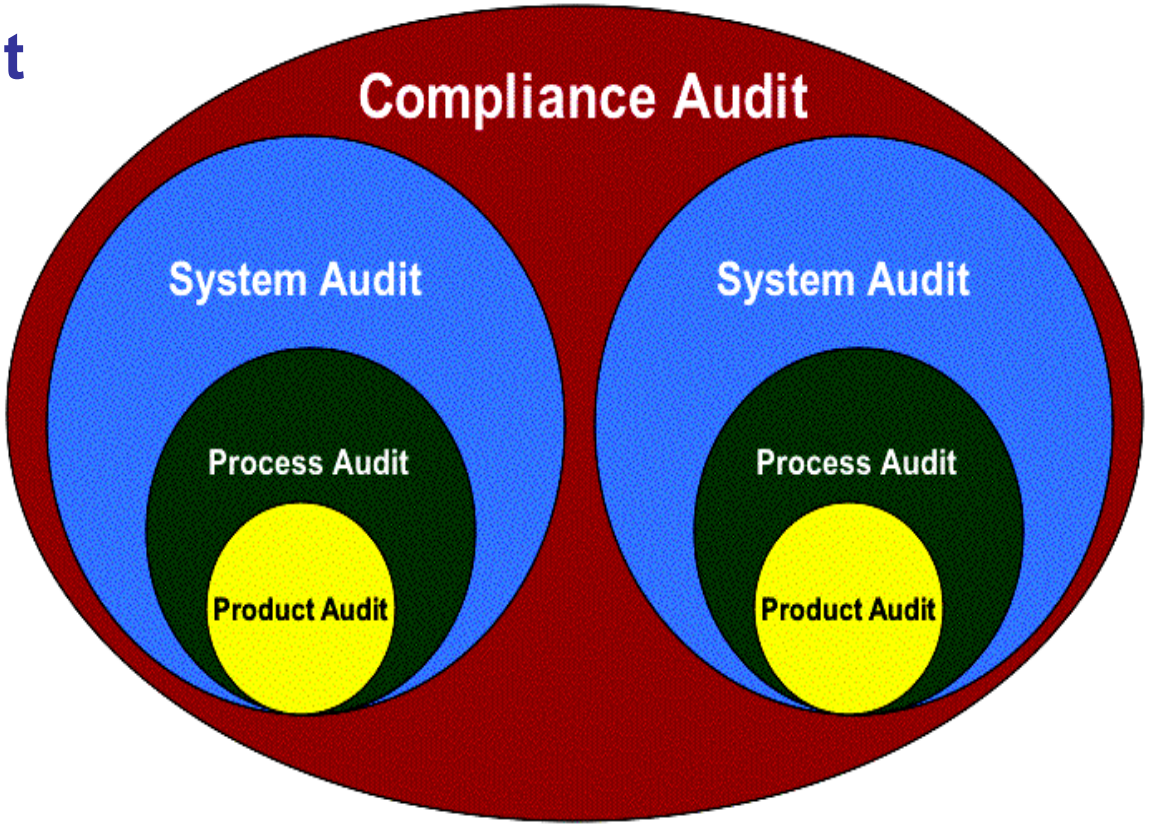
Auditi eesmärgiks on
objektiivsete andmete kogumine selleks, et anda põhjendatud hinnang auditeeritavate süsteemide seisundile

Auditi tüübid

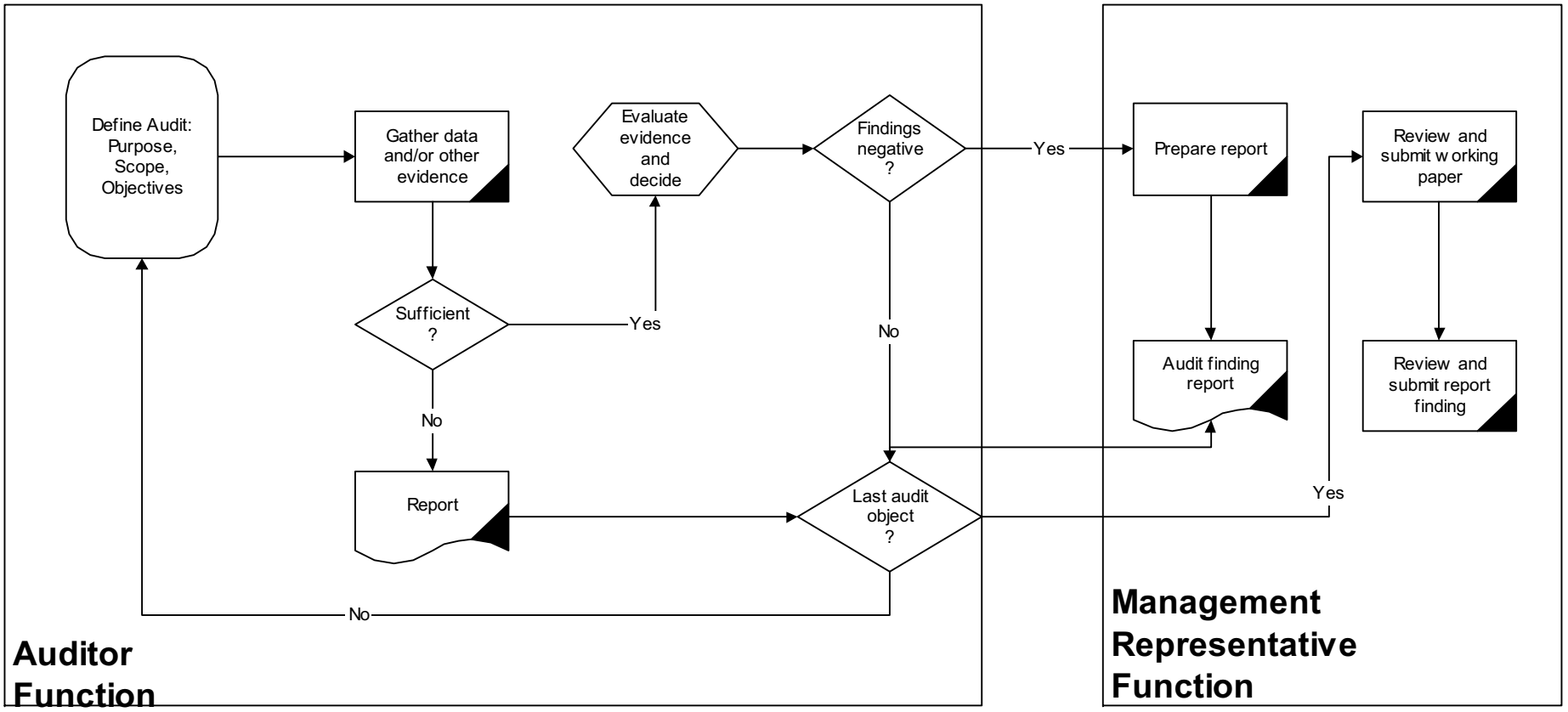
- **Siseaudit**
- **Välisaudit**
  - Teine osapool:
    - Klient auditeerib teenuse pakkujat
  - Kolmas osapool:
    - Audiitoriks on sõltumatu organisatsioon

Auditi alamtüübid

- **Vastavusaudit**
  - vastavus standarditele reeglitele, kordadele jne
- **Süsteemiaudit**
- **Protsessiaudit**
- **Tooteaudit**



Typical Audit System



Definitsioonid: *"kes"*

- **audiitor** – isik, kellel on vajalik kvalifikatsioon ja kes viib läbi auditi
- **klient** – auditit telliv isik või organisatsioon; siseauditi puhul – ettevõtte juhtkond
- **auditeeritav** – organisatsioon, süsteem, toode või isik, mida/keda auditeeritakse

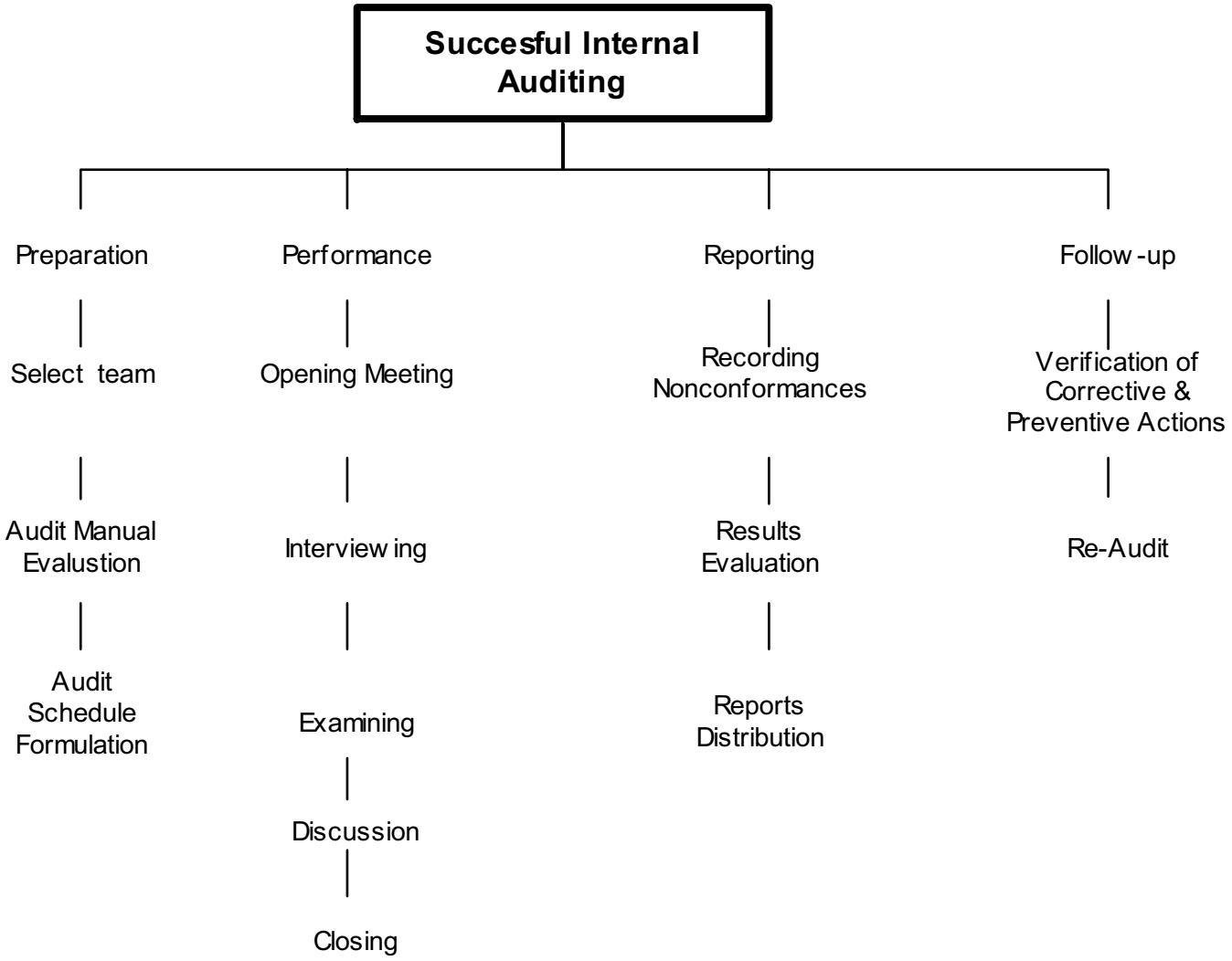
Definitsioonid: *“**mis**”*

- **Tähelepanek** – väide auditeerimisel leitud mittevastavuste kohta
- **Tõendus** – informatsioon auditeeritava objekti kohta, mida on võimalik tõestada
- **Mittevastavus** – auditeeritava objekti erinevus nõuetest

Auditi faasid

- Auditi plaanimine ja ettevalmistamine
- Auditi läbiviimine
- Auditi tulemuste aruanne (raport)
- Korrigeerivate toimingute määratlemine

Standard Four Phases



Auditi kava

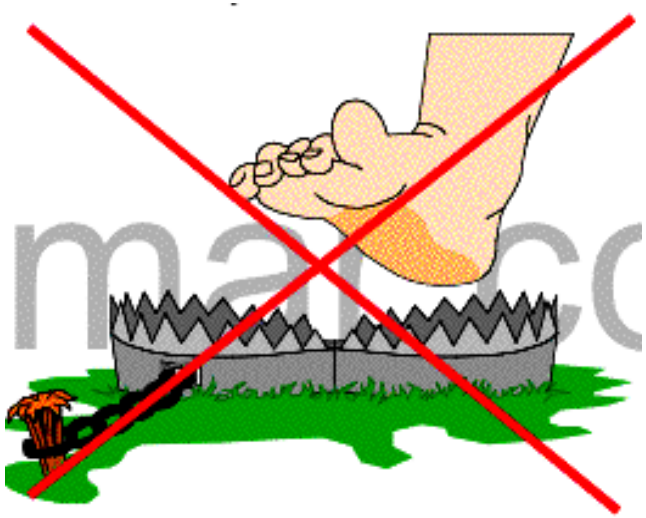
- Sissejuhatav kohtumine
- Info kogumine
- Mittevastavuste registreerimine
- Mittevastavuste hindamine
- Nõuetele vastavuse määratlemine
- Tähelepanekute fikseerimine
- Kokkuvõttev/lõpetav kohtumine

Tõendus

- Pole mõjutatud emotsioonidest ja/või eelarvamustest
- Põhineb vaatlusel
- On verbaalne või dokumenteeritud
- On verifitseeritav

Auditi vajadus

- Preventiivne toiming, leida probleemid varakult
- Juhtkonnale vajalik kontrollimehhanism
- Tagada süsteemide töö nõuete vastavalt
- Organisatsiooni parendamise mehhanism



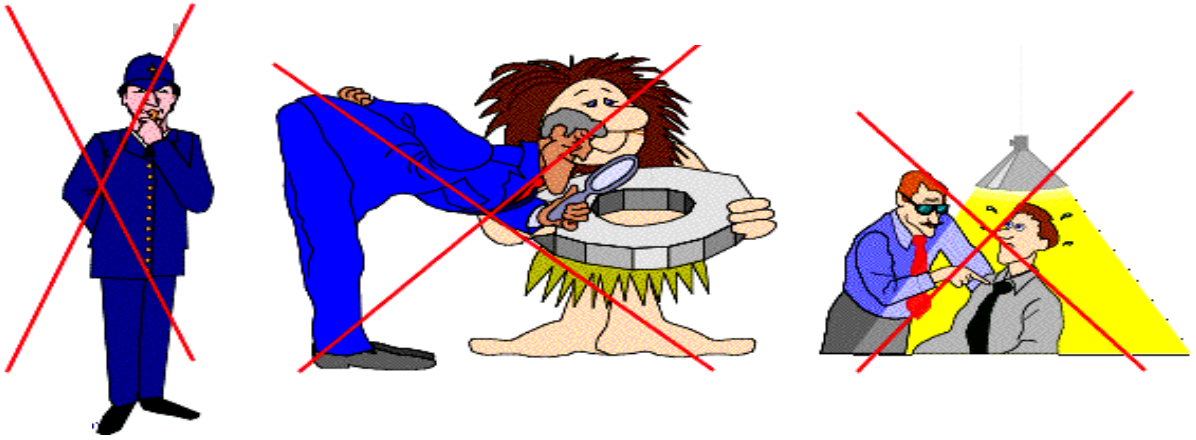
Audit peab olema

- avatud
- aus
- konstruktiivne

Auditeeritavale on audit alati kasulik

Auditorid pole

- Ebaausad
- Üliaktiivsed
- Urgitsejad
- Inkvisiitorid
- Politsei
- Karistus meie pattude eest



Auditi programm

- Tagab, et süsteemid rahuldavad dokumenteeritud nõudeid
- Tagab, et dokumenteeritud nõuded on praktilised, arusaadavad ja et neid järgitakse äriprotsessis
- Tagab auditi tulemuste fikseerimise – mittevastavused, korrektiivsed ja preventiivsed meetmed

Vastavusaudit
(*Complience Audit*)

Vastavusauditid

- Vastavusaudit kontrollib ettevõtte süsteemide vastavust auditi aluseks olevale standardile
- Üldiselt on kõik auditid suuremal või vähemal määral vastavusauditid
  - Näiteks, ka tooteauditi puhul määratletakse vastavust spetsifikatsioonile, joonisele jmt

Süsteemiaudit
(*Systems Audit*)

Süsteemiaudit

- Süsteemiaudit käsitleb ettevõtet süsteemsel tasemel
  - näiteks, ettevõtte süsteemide interaktsioon
- Tüüpilised süsteemiauditid:
  - Dokumentide kontroll
  - Testimisvahendid
  - Seirevahendid (monitooring)
  - Ründetõrjevahendid

Protsessiaudit
(*Process Audit*)

Protsessiaudit

- Protsessiaudit valideerib ettevõtte protsesse
- Protsessid on (enamasti) süsteemi osad – seega protsessiaudit on süsteemiauditi osa
- Protsessiaudit on sageli süsteemiauditi osa, kuid siseaudit võib auditeerida ka mõningaid protsesse eraldi
- Oluline on valideerida protsesside interaktsioonide tõhusust

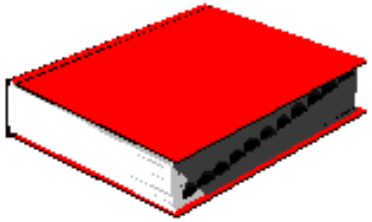
Tooteaudit
(*Product Audit*)

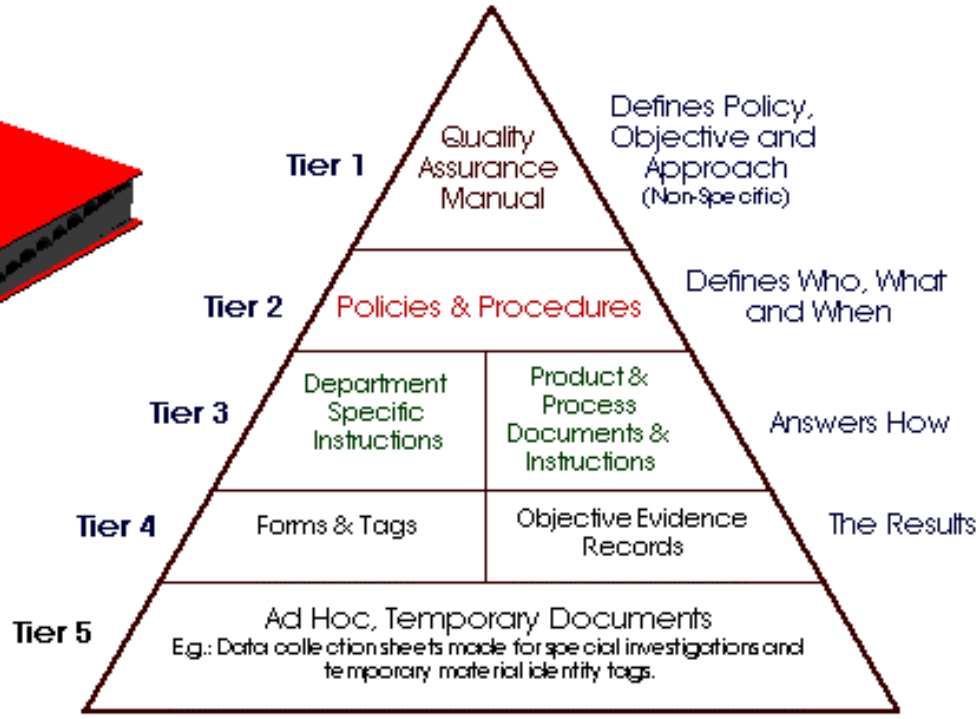
Tooteaudit

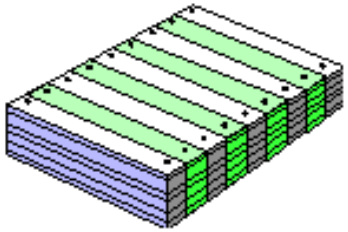
- Tooteaudit määratleb, kas (lõpp)toode või teenus vastab tema kasutuseesmärkidele, st. kas toode/teenus vastab nõuetele
- Tooteauditi võib teha:
  - klient
  - *harva* ka siseaudit

Mida auditeeritakse?

The Famed Document Pyramid



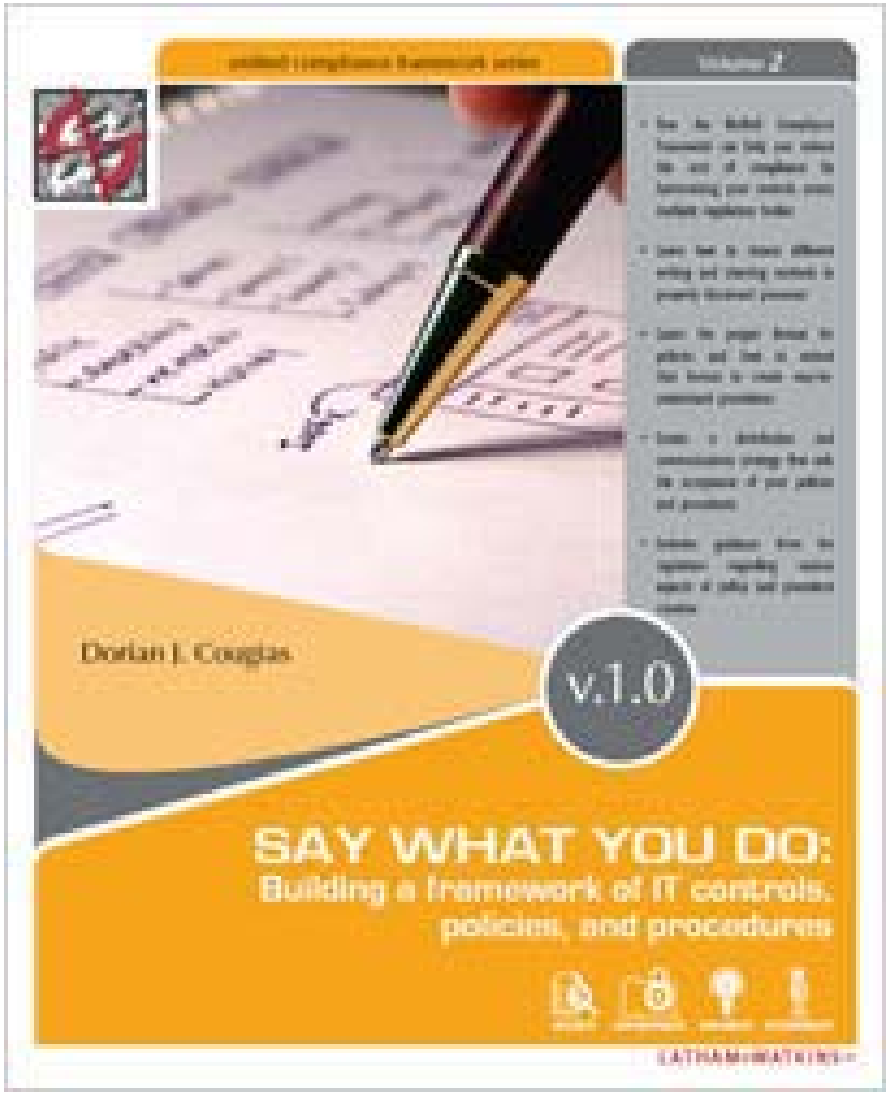




ISO/QS-9000
Quality Management System

- Dokumenteeri, mis teed
- Tee vastavalt dokumentatsioonile
- Registreeri, mis teed (jälg)
- *Say what you do and do what you say*

Say what you do



ISO 9001:2000	**Quality system.** **Say what you do.** **Do what you say.**

Protseduurid ja süsteemid

Protseduurid ja süsteemid

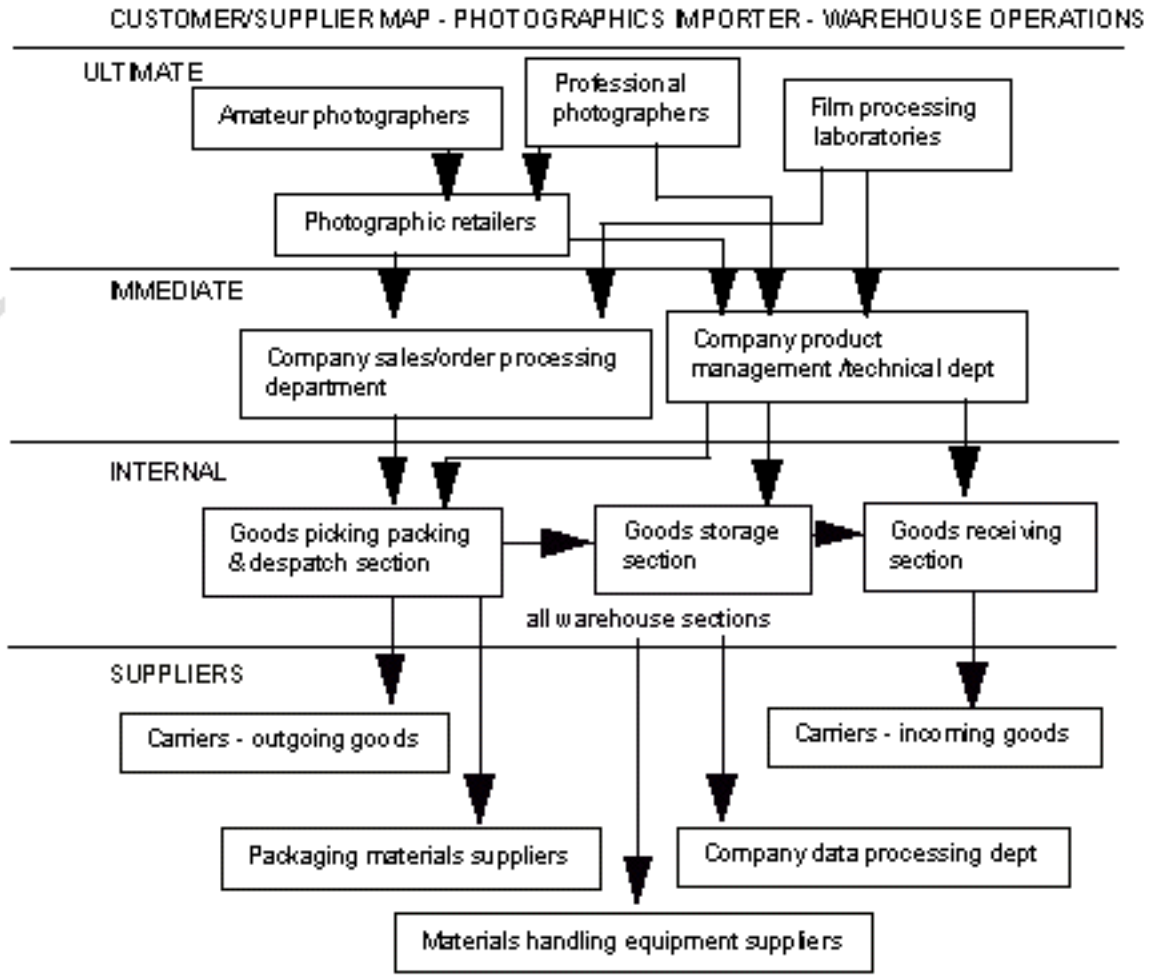
Dokumentatsiooni roll:

- Süsteemi dokumentatsioon
  - vs. NÕUDED
    - Mis sisaldub standardites jt dokumentides
  - vs. OBJEKTIIVSED LEIUD
    - Mis tegelikult toimub

Detailid

Keerulised ärisuhted

- Ettevõte ei eksisteeri vaakumis. Seosed on nii ettevõtte sees kui ka väliste partneritega



Olulised ja kriitilised protsessid

- Olulised protsessid
  - protsessid, mis tagavad organisatsiooni *oluliste* funktsioonide täitmise
  - on otseselt seotud kliendihuvide ja nõuete tagamisega
- Kriitilised protsessid
  - oluliste protsesside alamhulk
  - protsessid, mis tagavad organisatsiooni *eluliste* funktsioonide täitmise,
    st. nende protsesside katkemine pärsib organisatsiooni jätkusuutlikkuse

Vastutused

Kliendid vastutavad

- Määratlevad auditi eesmärgid ja vajadused ning algatavad auditeerimisprotsessi
- Määratlevad auditeeriva organisatsiooni
- Määratlevad auditi üldskoobi
- Saavad auditi raporti
- Määratlevad korrigeerivad toimingud (vajaduse korral)

Auditorid vastutavad

- Vastavus auditi nõuetega
- Auditi plaan
- Leidude dokumenteerimine
- Auditi tulemuste raport (aruanne)
- Korrigeerivate tomingute tõhususe verifitseerimine

Auditeeritavad vastutavad

- Töötajate informeerimine auditi eesmärkidest ja skoobist
- Vastutavate isikute määramine audiitoritega kohtumiseks
- Ressursside eraldamine audiitoritele nende töö toimivuse ja tõhususe tagamiseks
- Tagada audiitorite ligipääs kõigile vajalikele materjalidele ja isikutele
- Koostöö audiitoritega auditi eesmärkide saavutamiseks
- Korrigeerivate toimingute määratlemine ja algatamine

Audiitori omadused

- Haridus
- Kogemus
- Koolitus
- Pädevus
- Suhtlemisoskus

- Üldinformatsioon osakonnast
- Standardite hea tundmine

Auditi plaanimine

- Eesmärk
- Skoop
- Standardid ja juhendid
- Meeskond ja juht
- Auditi kestus
- Kontakt-osakonnad/isikud
- Määrata kuupäev ja kellaaeg
- Kontroll-list
- Konfidentsiaalsusnõuded

Auditi sagedus

- Auditeerimise sageduse määrab klient (va. nt. Finantsinspektsiooni audit)
- Auditi sageduse määramisel arvestatakse:
  - Eelmiste auditite tulemusi
  - Toimingu olulisust ja seisundit
  - Määratletud nõudeid
  - Olulisi muudatusi juhtimises, organisatsioonis, poliitikates, tehnoloogiates
  - Muudatusi süsteemis endas
- Siseaudit võib toimuda regulaarselt vastavalt juhtkonna otsusele

Kontroll-listid

Kontroll-listid

- Aitavad auditit planeerida
- Tagavad põhjalikkuse ja järjekindluse
- Määratlevad olulised kontroll-punktid
- Tüürivad auditit

Kontroll-listid – sisu

- Organisatsioon
- Vastutused/õigused
- Kvalifikatsioon/koolitus
- Mittevastavuse kontroll
- Leiud

Info kontroll-listideks

- Standardid
- Juhtkonna prioriteedid
- Sise- ja välisauditite aruanded
- Toote/protsessi info
- Piirangud

Dokumentide ülevaatus

- Tööprotseduuride vastavus standarditele
- Eelnevate audite korrigeerivad toimingud
- Kontroll-listide vormid
- Mõned küsimused:
  - Missugused on osakonna funktsioonid?
  - Missugused nendest funktsioonidest on olulised?

Auditi eelne teavitus

- Teavita aegsasti auditi toimumise ajast, kestusest, skoobist
- Veendu, et vajalikud töötajad on teavitatud